Multicam Digital Surveillance System

User's Manual V8.5.8.0

© 2013 Sting Alarm, Inc. All rights reserved.
Under the copyright laws, this manual may not be copied, in whole or in part, without the written consent of Sting Alarm.

Every effort has been made to ensure that the information in this manual is accurate. Sting Alarm, Inc. makes no expressed or implied warranty of any kind and assumes no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages arising from the use of the information or products contained herein. Features and specifications are subject to change without notice.

Trademarks used in this manual: *Sting Alarm*, the *Sting Alarm* logo and series products are trademarks of Sting Alarm, Inc. *Windows* and *Windows XP* are registered trademarks of Microsoft Corporation.

September 2013

Full Manual for
V8.5.8 Sting Alarm Surveillance System

Welcome to the Full Manual for V8.5.8 Sting Alarm Surveillance System.

Cards Supported

V8.5.8 Sting Alarm Surveillance System only supports the following video capture cards:

- -600(S) V3.20 and later
- -650(S) V3.30 and later
- -800(S) V3.30 and later
- -804A V3.10 and later
- -600A, -600B
- -650A, -650B
- -800A, -800B
- -900A
- -1120, -1120A, -1120B
- -1240, -1240A, -1240B
- -1480, -1480A, -1480B
- -3008
- -4008, -4008A
- -5016
- -SDI-204

Note that -600 (V4), -650 (V4) and -800 (V4) and -804 (V4) Cards are renamed to -600A, -650A, -800A and -804A. These V4 and A Cards are the same video capture cards.

Important Notes

GPU Decoding Specifications

In V8.5 or later, support for GPU (Graphics Processing Unit) decoding is added to lower the CPU loading and to increase the total frame rate supported by a -System. GPU decoding only supports the following software and hardware specifications:

Software Specifications

<table>
<tr><th colspan="2" rowspan="2"></th><th colspan="2">Supported</th><th rowspan="2">Not Supported</th></tr>
<tr><th>Sandy Bridge</th><th>Ivy Bridge / Haswell</th></tr>
<tr><td rowspan="2">Operating System</td><td>32-Bit</td><td colspan="2">Windows Vista / 7 / 8</td><td rowspan="2">Windows 2000 / XP / Server 2008</td></tr>
<tr><td>64-Bit</td><td>Windows 7 / 8 / Server 2008 R2 / Server 2012</td><td>Windows 7 / 8 / Server 2012</td></tr>
<tr><td colspan="2">-System</td><td>V8.5.0.0 or later</td><td>V8.5.8.0 or later</td><td></td></tr>
<tr><td colspan="2">Resolution</td><td>1 MP / 2 MP</td><td>1 MP / 2 MP / 3 MP / 4 MP / 5 MP</td><td>CIF / VGA / D1 / 4MP / 5MP</td></tr>
<tr><td colspan="2">Codec</td><td colspan="2">H.264</td><td>MPEG4 / MJEPG</td></tr>
<tr><td colspan="5">Note:
1. Windows 8 and Server 2012 are only supported in -System V8.5.7.0 or later.
2. To apply GPU decoding, the recommended memory (RAM) requirements is 4 GB Dual channels for 64-bit OS and 3 GB for 32-bit OS.</td></tr>
</table>

Hardware Specifications

<table>
<tr><td>Motherboard</td><td>Intel chipset with onboard VGA
Ex: Intel® Q87, Q85, B85, Z87, H87, H81, Q77, Q75, Z77, Z75, H77, B75, Q67, H67, H61, Q65, B65, Z68 Express Chipset.</td></tr>
<tr><td colspan="2">Note: If you want to use an external VGA card, it is required to connect a monitor to the onboard VGA to activate GPU decoding.</td></tr>
</table>

Multi-Channel Playback Specifications

In V8.5 or later, multi-channel playback in ViewLog has been enhanced to improve the smoothness of the video by producing higher frame rate. However, playing back multiple channels at high resolution can increase the CPU loading especially if the -System is processing other tasks simultaneously. As a result of the high CPU loading, dropped frames may sometimes occur in recorded video when playing back multiple megapixel channels.

To avoid the problem, **it is recommended to play back megapixel video in single view.**

Contents

1 Configuring Main System 4

1.1 Getting Started 4

1.1.1 Main Screen 6

1.1.2 Installing Cameras 8

1.1.3 Enabling the Recording 9

1.1.4 Playing Back Video 10

1.2 System Configuration 11

1.2.1 General Setting 11

1.2.2 Setting Data Storage 15

1.2.3 Adjusting Camera Configuration 18

1.2.4 Setting Day and Night Recording Mode 23

1.2.5 Geo Mpeg4 Advanced Settings 24

1.2.6 Customizing Startup Settings 26

1.2.7 Customizing Display Settings 28

1.2.8 Setting Auto Reboot 30

1.2.9 Setting Text Overlay 31

1.3 Audio and Video Settings 33

1.3.1 Setting Video Source and Resolution 33

1.3.2 Fixing Aspect Ratio 34

1.3.3 Adjusting Video Attributes 35

1.3.4 Adjusting Audio Setting 39

1.3.5 Turbo Mode 41

1.4 Camera Monitoring 43

1.4.1 Snapshot 43

1.4.2 Associate Monitoring 44

1.4.3 Daylight Saving Time Recording 46

1.5 Account and Password 48

1.5.1 Creating an User Account 49

1.5.2 Changing Password on Login 51

1.5.3 Retrieving Password Through E-mail 52

1.5.4 Preventing Unauthorized System Termination 53

1.5.5 Setting Double Passwords for ViewLog Access 54

1.6 System Idle Protection 55
1.6.1 Auto Logout Administrator 55
1.6.2 Auto Login User without Access Rights 56
1.6.3 Auto Start Recording 57
1.7 System Log 58
1.7.1 Viewing Event Logs 58
1.7.2 Setting Event Logs 63
1.7.3 Searching Event Logs 65
1.8 Recording Schedule 66
1.8.1 Video Schedule 67
1.8.2 Special Days Schedule 69
1.8.3 I/O Schedule 70
1.8.4 Center V2 Schedule 71
1.9 Schedule Center 72
1.9.1 Compacting Video Events 72
1.9.2 Merging Video Events 76
1.9.3 Setting Backup Schedule 79
1.9.4 Setting VSM Schedule 81
1.10 Alert Notification 83
1.10.1 Setting Email Server 85
1.10.2 Setting Hotline Services 87
1.11 PTZ Control 89
1.11.1 Mapping PTZ Cameras 91
1.11.2 PTZ Idle Protection 92
1.11.3 Auto Switching PTZ Control Panels 94
1.11.4 PTZ Automation 95
1.12 Digital PTZ Control 97
1.13 Pop-up Live Video 99
1.14 Video Noise Solutions 100
1.14.1 Noise Tolerance 100
1.14.2 Noise Detection to Reduce File Size 102
1.14.3 Noise Filter 103
1.15 Picture-in-Picture View 104
1.16 Picture-and-Picture View 105
1.17 Shortcuts 105
1.18 Touch Screen Support 107
1.18.1 PTZ and I/O Control Panel 107
1.18.2 Touch Screen Panel 107

1.19 System Tools 109
1.19.1 Hard Disk Calculator 109
1.19.2 Colorful Mode 111
1.19.3 Stopping Video Lost Watchdog 111
1.19.4 Deactivating Video Lost Beep 112
1.19.5 Fast Key Lockup 112
1.19.6 Fast Key Reference 113
1.19.7 Network Failure Detection 113
1.19.8 Memory Limit 114
1.19.9 Version Information 114

2 Hybrid and NVR Solution 116

2.1 Sting Alarm IP Video Products 116
2.2 Dongle Requirement 117
2.3 Hybrid Solution Description 118
2.4 NVR Solution Description 119
2.5 IP Channel Setup 120
2.5.1 Adding Cameras Manually 121
2.5.2 Scanning Camera 123
2.5.3 Automatic Setup 124
2.5.4 Customizing IP Camera Settings 125
2.6 PTZ IP Camera 127
2.7 RTSP Connection 128
2.8 ONVIF & PSIA Connection 130
2.8.1 ONVIF Connection 130
2.5.4 PSIA Connection 132
2.9 Camera Mapping Using IP Device Utility 133
2.10 Economic Mode 135
2.11 On Demand Display 138

3 Video Analysis 142

3.1 Object Tracking and Zooming 142

3.1.1 Object Tracking 142

3.1.2 Object Zooming 149

3.2 Advanced Single Camera Tracking 152

3.3 Digital Object Tracking 155

3.3.1 Setting Digital Object Tracking 155

3.3.2 Tracking in PIP View 157

3.3.3 Tracking in PAP View 158

3.4 Object Counting and Intrusion Alarm 159

3.4.1 Object Counting 160

3.4.2 Intrusion Alarm 164

3.5 Object Index 168

3.5.1 Setting Object Index 168

3.5.2 Viewing Object Index 170

3.5.3 Searching Object Index 171

3.6 Automatic Video Snapshots 173

3.6.1 Setting Video Snapshots 173

3.6.2 Searching Video Snapshots 175

3.7 Face Detection 177

3.8 Face Count 179

3.8.1 Installing the Camera 179

3.8.2 Setting Face Count 180

3.9 Unattended and Missing Object Detection 183

3.9.1 Detecting Unattended Objects 183

3.9.2 Detecting Missing Objects 185

3.10 Privacy Mask Protection 188

3.10.1 Setting a Privacy Mask 188

3.10.2 Granting Access Privileges to Recoverable Areas 189

3.11 Scene Change Detection 190

3.12 Panorama View 192

3.12.1 Stitching a Panorama View with Overlapping Areas 194

3.12.2 Easy Mode with No Overlapping Area 195

3.12.3 Accessing a Panorama View 198

3.13 Video Defogging 199
3.14 Video Stabilization 201
3.15 Wide Angle Lens Dewarping 203
3.16 Advanced Motion Detection 205
3.17 Crowd Detection 202
3.18 Advanced Scene Change Detection 210
3.19 Advanced Unattended Object Detection 213
3.20 Advanced Missing Object Detection 216
3.21 Video Analysis Schedule 219
3.21.1 Privacy Mask Schedule 221
3.22 Fisheye View 222
3.22.1 Setting Up a -Fisheye Camera 223
3.22.2 Setting Up a Third-Party Fisheye Camera 225
3.22.3 Object Tracking 225
3.23 Specifications 229

4 Video Playback 232

4.1 Playing Back on ViewLog 233
4.1.1 Playback Screen Layout 236
4.1.2 Playback Control Buttons 238
4.1.3 Recycling Option for Video Files 240
4.1.4 Bookmarking a Frame 241
4.1.5 Searching a Video Event 243
4.1.6 Merging and Exporting Video 248
4.1.7 Extracting Frames from a Video Event 255
4.1.8 Saving Images 256
4.1.9 Printing Images 257
4.1.10 Setting Face Mask 259
4.1.11 Displaying GPS Data 261
4.1.12 Adjusting Distorted Views 262
4.1.13 Object Tracking in Fisheye View 263
4.1.14 Event Search Limitation 265
4.1.15 Advanced Settings 266

4.2 Object Search 274

4.3 Advanced Log Browser 277
4.3.1 Filter Settings 279
4.4 Quick Search 281
4.4.1 Event Query Settings 283
4.4.2 Advanced Search Settings 284
4.5 Address Book 285
4.5.1 Creating a Host Account 285
4.5.2 Creating a Group 286
4.5.3 Creating a Folder Link 287
4.5.4 Connecting from Address Book 288
4.5.5 Importing and Exporting the Address Book 289
4.6 Remote ViewLog Service 290
4.6.1 Retrieving Recordings from a Single Host 290
4.6.2 Retrieving Recordings from Multiple Hosts 291
4.6.3 Retrieving Images of Object Index 292
4.6.4 Resuming Backup 293
4.7 Single Player 294
4.7.1 Single Player Window 294
4.8 GPS Tracks Playback 296
4.9 Touch Screen Support 298
4.10 Fast Key Reference 299
4.11 Specifications 299

5 Backup, Deletion and Repair 301

5.1 Backing Up Log Data 301
5.2 Backing Up Recorded Files 303
5.3 Splitting Backup Files onto Multiple Discs 306
5.3.1 Excluding the Player in the Backup Files 306
5.3.2 Including the Player in the Backup Files 308
5.4 Deleting Recorded Files 309
5.5 Repairing Damaged File Paths 311
5.6 Repairing Damaged Video Files 313

6 I/O Applications 316

6.1 I/O Device Setup 317

6.1.1 Latch Trigger 319

6.1.2 Keeping Last Toggle Status 321

6.2 I/O Control Panel 323

6.3 Advanced I/O Applications 324

6.3.1 Setting Up Actions Upon Input Trigger 325

6.3.2 Moving PTZ Camera to a Preset Location upon Input Trigger 327

6.3.3 Setting Momentary and Maintained Modes 328

6.3.4 Deactivating Alarm and Alert Settings upon Input Trigger 329

6.3.5 Overlaying Input Name onto Screen upon Input Trigger 330

6.4 Input State Detection 331

6.5 I/O Enable Setting 332

6.6 Advanced I/O Panel 333

6.6.1 The Advanced I/O Panel 333

6.6.2 Creating a Group for Cascade Triggers 334

6.6.3 Configuring the Advanced I/O Panel 337

6.6.4 Setting Up Mode Schedule 338

6.6.5 Quick Link 340

6.6.6 Forcing Output 341

6.6.7 Editing Background Image 342

6.6.8 System-Wide Triggers 343

6.6.9 The “Advanced Logical Input Status in Multicam” Option 344

6.6.10 Managing a Group of I/O Devices 345

6.7 Visual Automation 346

6.7.1 Setting Visual Automation 346

6.7.2 Using Visual Automation 347

6.8 Virtual I/O Control 348

6.8.1 Setting a Module 349

7 Point-Of-Sale (POS) Application..... 351

7.1 Text-Mode POS Device 351
7.1.1 Windows-Based Direct POS Integration 351
7.1.2 Data Capture Box Integration 356
7.2 Graphic-Mode POS Device 357
7.2.1 Serial Port Connection 357
7.2.2 Network Connection 359
7.3 POS Device Setup 361
7.4 POS Data Overlay 363
7.5 POS Field Filter 365
7.6 Abnormal Transaction Alerts 367
7.6.1 Setting Alarm Frequency 368
7.7 Codepage Mapping 370
7.8 POS Data Search 371
7.9 POS Live View 372
7.9.1 The POS Live View Window 372
7.9.2 Setting Live View 373
7.10 POS Color Text 374
7.10.1 Setting POS Color Text 374

8 Remote Viewing..... 379

8.1 Remote Viewing Using a Web Browser 380
8.2 WebCam Server Settings 384
8.2.1 General Settings 384
8.2.2 Server Settings 385
8.2.3 Video Settings 386
8.2.4 SDK Settings 387
8.2.5 Audio Settings 388
8.2.6 JPG Settings 390
8.2.7 3GPP Settings 391
8.2.8 Mobile Settings 392

8.2.9 Multicast Settings 393
8.2.10 UPnP Settings 394
8.2.11 FTP Server Settings 397
8.2.12 Network Port Information 398
8.3 Single View Viewer 399
8.3.1 Control Panel 401
8.3.2 Server List 402
8.3.3 Video Recording 403
8.3.4 Alarm Notification 404
8.3.5 Video and Audio Configuration 405
8.3.6 Hardware-Compressed or Megapixel Stream 407
8.3.7 PTZ Control 408
8.3.8 Visual PTZ Control Panel 409
8.3.9 I/O Control 410
8.3.10 Visual Automation 411
8.3.11 Picture-in-Picture View 412
8.3.12 Picture-and-Picture View 413
8.3.13 Image Enhancement 414
8.3.14 Remote Configuration 415
8.4 2-Window Viewer 417
8.5 Multi-Window Viewer 418
8.6 Multi View Viewer 419
8.6.1 Installation of Multi View 419
8.6.2 Host List 423
8.6.3 Channel Status Information 424
8.6.4 Creation of a Host 425
8.6.5 Combination of Multiple Hosts into a Single Host 426
8.6.6 Video Recording 428
8.6.7 Camera Polling 429
8.6.8 Hardware-Compressed or Megapixel Stream 430
8.6.9 PTZ Control 431
8.6.10 Visual PTZ Control Panel 432
8.6.11 Output Control 433
8.6.12 Remote ViewLog 434
8.6.13 System Configuration 435
8.6.14 Camera Status 437
8.6.15 Host Information 438
8.6.16 Icon Image Change 439

8.7 Multicast and Audio Broadcast 440
8.7.1 Configuring Multicast and Broadcast Settings 440
8.7.2 Sending Audio Broadcast 442
8.7.3 Receiving Multicast and Audio Broadcast 443
8.8 JPEG Image Viewer 445
8.9 Remote Playback 446
8.10 Remote ViewLog 447
8.11 Event List Query 448
8.12 Download Center 450
8.13 Mobile Phone Applications 451
8.13.1 iPhone, iPod Touch, and iPad 452
8.13.2 Android Smartphones and Tablets 455
8.14 Web Browsers on Smartphones 459

9 E-Map Application 463

9.1 The E-Map Editor 463
9.1.1 The E-Map Editor Window 464
9.2 Creating an E-Map File 465
9.2.1 Creating an E-Map File for a Remote Host 467
9.2.2 Setting Polygonal Map to Locate a Triggered Device 468
9.2.3 Setting View Zone to Show the Monitored Area 469
9.3 Starting E-Map 470
9.3.1 Setting the Pop-up Map Function 471
9.4 Starting E-Map from a Remote Site 472
9.4.1 The Remote E-Map Window 472
9.4.2 Logging in Different Hosts 474
9.4.3 Configuring the Remote E-Map 475
9.4.4 Viewing Host Information and Playing Back Video 476
9.4.5 Accessing Remote ViewLog 477
9.5 E-Map Server 478
9.5.1 Installing E-Map Server 478
9.5.2 The E-Map Server Window 479
9.5.3 Setting E-Map Server 480
9.5.4 Remote Monitoring via E-Map Server 481
9.5.5 Accessing Authentication Server Account Information 482

10 Short Message Service 484

10.1 Installing SMS Server 484
10.2 The SMS Server Window 485
10.3 SMS Server Setup 486
10.3.1 Device Settings 486
10.3.2 Server Settings 487
10.3.3 Account Settings 490
10.4 SMS Log 492
10.4.1 Setting SMS Log 492
10.4.2 Viewing SMS Log 493
10.5 Password Security 495
10.6 SMS Notification 495
10.6.1 Connecting -System to SMS Server 495
10.6.2 Setting Mobile Numbers 497
10.6.3 Setting Alert Notification 498

11 Useful Utilities 502

11.1 Dynamic DNS 502
11.1.1 Installing Dynamic DNS 503
11.1.2 Registering Domain Name with DDNS 504
11.1.3 Starting Dynamic DNS 506
11.1.4 Local DDNS Server 508
11.2 Watermark Viewer 509
11.2.1 Activating Watermark Protection 509
11.2.2 Running the Watermark Proof 510
11.2.3 The Watermark Proof Window 511
11.3 Twin View Display 512

11.4 Windows Lockup 514
11.4.1 The -Desktop Screen 514
11.4.2 -Desktop Features 515
11.4.3 Token File for Save Mode 518
11.5 Authentication Server 519
11.5.1 Installing the Server 519
11.5.2 The Server Window 520
11.5.3 Creating a Client DVR 521
11.5.4 Creating a User Account 522
11.5.5 Importing Groups and Users from Active Directory 523
11.5.6 Starting the Server 525
11.5.7 Connecting -System to the Server 527
11.5.8 Remote Access from Control Center, Remote E-Map and MultiView 530
11.6 Fast Backup and Restore 533
11.6.1 Installing the FBR Program 533
11.6.2 Customizing Logo and Button 534
11.6.3 Customizing the Features 535
11.6.4 Backing up and Restoring Settings 536
11.7 Hot-Swap Recording 538
11.7.1 The Media Man Tool Window 539
11.7.2 Viewing Disk Drive Status 540
11.7.3 Adding a Disk Drive 542
11.7.4 Removing a Disk Drive 543
11.7.5 Logging In Automatically at Startup 544
11.7.6 Setting LED Panel 545
11.8 Backup Server 547
11.8.1 Adding a Disk Volume 547
11.8.2 Enabling Backup Server 549
11.8.3 Advanced Settings 550
11.8.4 Manually Adding Files for Backup 553
11.8.5 Viewing Server Status 554
11.8.6 Retrieving Recorded Files 556
11.8.7 Viewing Backup Status 557
11.9 Backup Viewer 558
11.9.1 Usage Requirements 558
11.9.2 Starting Backup Viewer 559
11.9.3 Performing Queries 560

11.9.4 Viewing the Event Files 561
11.9.5 Using Remote ViewLog 562
11.10 Bandwidth Control Application 563
11.10.1 Installing the Bandwidth Control 564
11.10.2 Allowing Remote Control at DVR 565
11.10.3 Connecting to a WebCam Server 566
11.10.4 Controlling a WebCam Server 567
11.10.5 Bandwidth Setup 568
11.10.6 Block List Setup 569
11.10.7 General Setup 570
11.11 Report Generator 571
11.11.1 Starting Report Generator 571
11.11.2 Setting Report Generator 572
11.11.3 Setting Report Criteria 574
11.11.4 E-Mail Attachment Settings 577
11.11.5 Playing Back Video Recordings 578
11.11.6 Viewing Event Log 580
11.12 Spot Monitor Controller 581
11.12.1 Spot Monitor Controller 581
11.12.2 Spot Monitor Panel 584
11.13 Quad Spot Monitor Controller 585
11.13.1 Setting the Controller 585
11.13.2 Setting Pop-up Views 588
11.13.3 Displaying TV Quad Panel 589
11.14 Digital Matrix 590
11.14.1 Activating Multiple Monitors 590
11.14.2 Setting Live View 592
11.14.3 Setting Scanned Pages 593
11.14.4 Setting Pop-up Alert 594
11.14.5 Setting Live View with Pop-up Alert 596
11.14.6 Controlling Screen Display 597
11.15 GIS Recording 598
11.15.1 Setting the GPS Receiver 598
11.15.2 Recording GPS Locations of -System 600
11.15.3 Recording GPS Locations of the IP Device 601
11.15.4 Viewing GPS Locations during Playback 602
11.15.5 Sending GPS Data to the -GIS 604

11.16 -IP Device Utility 607
11.16.1 Installing -IP Device Utility 607
11.16.2 The -IP Device Utility Window 608
11.16.3 Setting IP Devices 609
11.16.4 Mapping IP Cameras 610
11.17 MCamCtrl Utility for -Joystick 611
11.17.1 Installing MCamCtrl Utility 611
11.17.2 Starting the MCamCtrl Utility 612
11.18 -Mobile Server 613
11.19 Language Setting 614
11.19.1 MultiLang Tool for Translated Text 614
11.19.2 SetLanguage Tool to Set UI Language 618
11.20 Skype Video Utility 619
11.20.1 Installing -Skype Video Utility 620
11.20.2 Setting Up Notifications Upon Motion or I/O Trigger 621

Appendix 629

A. USB Dongle Required for IP Device Applications 629
B. Supported PTZ Protocols and Models 630
C. Certified PTZ Models for Object Tracking 632
D. Certificated PTZ Models for Full Degree Pan and Tilt Control 633
E. Supported IP Device Brands 634
F. Supported GPRS Models 635
G. Custom Icon Naming Chart for Multi View 636
H. Display Ratio Supported by Panel Resolution 637
I. Dual Stream Support List 638

Chapter 1

Configuring Main System.....4

1.1 Getting Started 4

1.1.1 Main Screen 6
1.1.2 Installing Cameras 8
1.1.3 Enabling the Recording 9
1.1.4 Playing Back Video 10

1.2 System Configuration 11

1.2.1 General Setting 11
1.2.2 Setting Data Storage 15
1.2.3 Adjusting Camera Configuration 18
1.2.4 Setting Day and Night Recording Mode 23
1.2.5 Geo Mpeg4 Advanced Settings 24
1.2.6 Customizing Startup Settings 26
1.2.7 Customizing Display Settings 28
1.2.8 Setting Auto Reboot 30
1.2.9 Setting Text Overlay 31

1.3 Audio and Video Settings 33

1.3.1 Setting Video Source and Resolution 33
1.3.2 Fixing Aspect Ratio 34
1.3.3 Adjusting Video Attributes 35
1.3.4 Adjusting Audio Setting 39
1.3.5 Turbo Mode 41

1.4 Camera Monitoring 43

1.4.1 Snapshot 43
1.4.2 Associate Monitoring 44
1.4.3 Daylight Saving Time Recording 46

1.5 Account and Password 48

1.5.1 Creating an User Account 49
1.5.2 Changing Password on Login 51
1.5.3 Retrieving Password Through E-mail 52
1.5.4 Preventing Unauthorized System Termination 53
1.5.5 Setting Double Passwords for ViewLog Access 54

1.6 System Idle Protection 55

1.6.1 Auto Logout Administrator 55

1.6.2 Auto Login User without Access Rights 56

1.6.3 Auto Start Recording 57

1.7 System Log 58

1.7.1 Viewing Event Logs 58

1.7.2 Setting Event Logs 63

1.7.3 Searching Event Logs 65

1.8 Recording Schedule 66

1.8.1 Video Schedule 67

1.8.2 Special Days Schedule 69

1.8.3 I/O Schedule 70

1.8.4 Center V2 Schedule 71

1.9 Schedule Center 72

1.9.1 Compacting Video Events 72

1.9.2 Merging Video Events 76

1.9.3 Setting Backup Schedule 79

1.9.4 Setting VSM Schedule 81

1.10 Alert Notification 83

1.10.1 Setting Email Server 85

1.10.2 Setting Hotline Services 87

1.11 PTZ Control 89

1.11.1 Mapping PTZ Cameras 91

1.11.2 PTZ Idle Protection 92

1.11.3 Auto Switching PTZ Control Panels 94

1.11.4 PTZ Automation 95

1.12 Digital PTZ Control 97

1.13 Pop-up Live Video..... 979

1.14 Video Noise Solutions 100

1.14.1 Noise Tolerance 100

1.14.2 Noise Detection to Reduce File Size 102

1.14.3 Noise Filter 103

1.15 Picture-in-Picture View..... 104

1.16 Picture-and-Picture View 105

1.17 Shortcuts 106

1.18 Touch Screen Support 107

1.18.1 PTZ and I/O Control Panel 107

1.18.2 Touch Screen Panel 107

1.19 System Tools 109

1.19.1 Hard Disk Calculator 109

1.19.2 Colorful Mode 111

1.19.3 Stopping Video Lost Watchdog 111

1.19.4 Deactivating Video Lost Beep 112

1.19.5 Fast Key Lockup 112

1.19.6 Fast Key Reference 113

1.19.7 Network Failure Detection 114

1.19.8 Memory Limit 1144

1.19.9 Version Information 1144

CHAPTER

1

Configuring Main System

1.1 Getting Started

When you start the system for the first time, the system will prompt you for a Supervisor ID and Password.

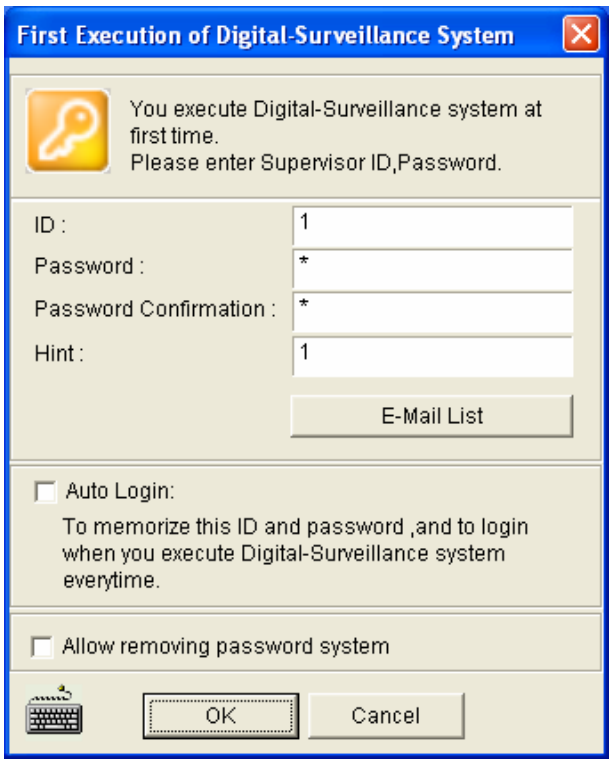


Figure 1-1

1. Type an ID and a password. Type the password again for confirmation.
2. Type a hint that would remind you of the password when the password you entered is incorrect.
3. It is recommended to click **E-Mail List** and enter e-mail addresses. When you forget the password, the password can be sent to your e-mail account.
4. Click **OK** to enter the main screen. You can also select the following options:

   ④ **Auto Login:** Allows auto login as the current user every time when the system is launched. For security purposes, this feature is only recommended for single-user systems.

④ **Allow removing password System:** It is recommended to select this option which allows removing the password database once you forget passwords. For details, see the same option in *Account and Password* later in this chapter.

④ : Click to open the onscreen keyboard and enter the login information.

1.1.1 Main Screen

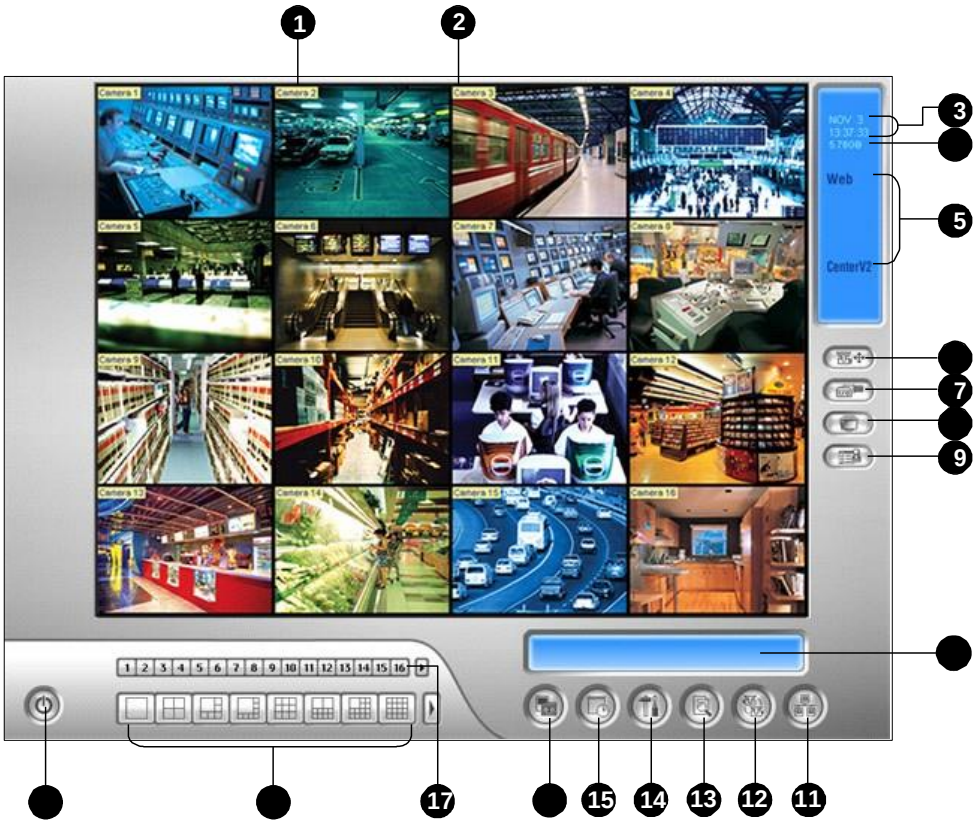


Figure 1-2

The controls in the main screen:

No.	Name	Description
1	Camera Number	Indicates the camera number matching the port number in the video capture card.
2	Camera Name	Indicates the given camera name.
3	Date/Time	Displays the current date and time.
4	Storage Space	Indicates the remaining disk space.
5	Connection	Indicates the connection status of remote applications.
6	PTZ Control	Displays the PTZ control panel.
7	I/O Control	Displays the I/O control panel.
8	TV-Out	Displays the TV Quad control panel.
9	User-Defined	Accesses other applications.
10	Location Name	Indicates the -System's name, usually named by its geographical location.

11	Network	Enables the connection to remote applications.
12	Camera Scan	Rotates through the screen divisions.
13	ViewLog	Brings up these options: Video/Audio Log, System Log, Search POS Data, POS Live View, Live Object Index, Search Object Index and E-Map.
14	Configure	Accesses System settings.
15	Schedule	Set up recording schedule.
16	Monitor	Starts monitoring.
17	Camera Select	Select the desired camera number for main division view.
18	Screen Division	Select screen divisions.
19	Exit	Brings up these options: Login/Change User, Logout, Minimize, Restart Multicam and Exit.

1.1.2 Installing Cameras

To set up cameras on the -System, click the **Configure** button (No.14, Figure 1-2), select **System Configure** and click **Camera Install**.

- ⌘ If you are connecting to an IP camera, select **IP Camera Install** and refer to *IP Channel Setup* in Chapter 2 for detailed instructions.
- ⌘ For analog cameras, no further configuration is required after physically installing the cameras. To disable a connected camera, select **Camera Install**. In the dialog box, clear the checkmarks of the channels you want to disable and click **OK**.

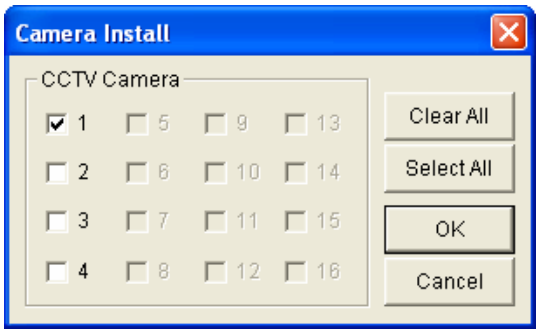


Figure 1-3

1.1.3 Enabling the Recording

To start recording, press **[F7]** on the keyboard, or click the **Monitor** button (No. 16, Figure 1-2) and select a camera. By default, every camera records with the following settings:

Default Recording Settings	
Recording Mode	Motion Detection
Resolution	320 x 240
Codec	Geo Mpeg4

When working with the system, you will undoubtedly want to change the settings as you go along. The buttons on the main screen provide quick access to several popular Main System settings. Click any button to see the menus of these settings.

- To change **recording mode**, see *Monitor Control* in *Adjusting Individual Camera* later in this chapter.
- To change **resolution**, first you need to set up video source and resolution of your system (see *Setting Video Source and Resolution* later in this chapter) and then define the resolution of each camera (see *Resolution Button* in *Adjusting Individual Camera* later in this chapter.)
- To change **codec**, see *Recording Code* in *Adjusting Individual Camera* later in this chapter.

1.1.4 Playing Back Video

You can instantly play back the recorded video of a certain time length without interrupting the monitoring and recording.

- ⌘ To instantly play back the events of one single channel, click on the **Camera Name** (No. 2, Figure 1-2), and select the time length.
- ⌘ To instantly play back the events of all channels, click on the **ViewLog** button (No. 13, Figure 1-2), select **Instant Play**, and select the time length.

Time length choices include 10 seconds, 30 seconds, 1 minute and 5 minutes.

Note: For details on the ViewLog player, see *Video Playback* in Chapter 4.

1.2 System Configuration

This section introduces system configurations of the -System.

1.2.1 General Setting

Let's start with the options on the General Setting dialog box. Changes made on the **General Setting** dialog box would apply to all available cameras attached to the system. Click the **Configure** button (No.14, Figure 1-2), select **System Configure**, and click **General Setting** to access the following dialog box.

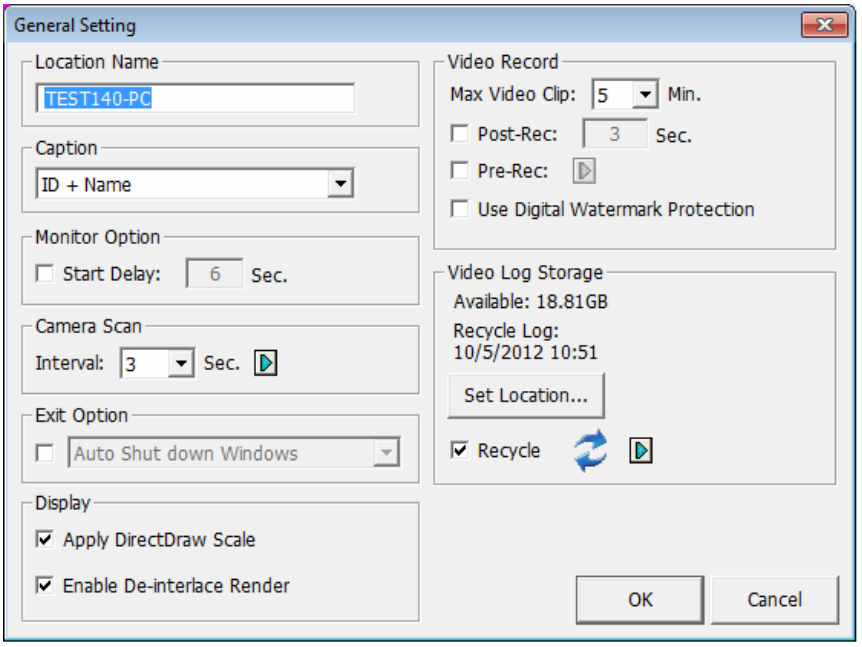


Figure 1-4

[Location Name] The given name (maximum 14 characters) is displayed in main screen as the name of the server.

[Caption] Display camera ID and name on the upper left-hand corner of the camera screen. You may choose **No** for no caption; **ID** to show only camera ID; **ID+Name** to show both camera ID + Name.

[Monitor Option] Select **Start Delay** to start recording after x second(s) when the system is activated.

[Camera Scan] When rotating through screen divisions, -System will switch to the next screen division after the time specified in the drop-down list elapses.

[Exit Option]

- ④ **Auto Shutdown Windows:** Closes Windows OS after exiting -System.
- ④ **Auto Restart Windows:** Restarts Windows OS after exiting -System.

[Display]

- ④ **Enable DirectDraw Scale:** Applies DirectDraw Scale to enhance image quality if your VGA card supports it. For certain VGA cards, DirectDraw Scale can result in blurred images. To avoid the image problem and remain DirectDraw Scale, change the image quality from High to Standard. See *Image Quality of DirectDraw Scale* in *System Tools* later in this chapter.
- ④ **Enable De-interlace Render:** Avoids interlace of the odd and even video lines. This feature affects only single view mode with the resolution of 640 x 480 and 704 x 480. After enabling the feature, you must restart the -System to apply it.

Note: The **Enable Directdraw Scale** and **De-interlace Render** features can greatly enhance image quality. If your VGA card supports DirectX9, enable both settings.

Tip: To check the version of your DirectX, search for the file name **dxdiag**. Open the file and find the related information.

[Video Record]

- ④ **Max Video Clip:** Specifies the maximum time length of each recorded file (from 1 to 5 minutes). If you select **5 Min**, a 30-minute event will be chopped into six 5-minute event files; if you select **1 Min**, a 30-minute event will be chopped into thirty 1-minute event files. To decide what to set up here, consider how often you back up your event files, and how intensive the activity is in your surveillance area. Smaller file size makes backup process faster.
- ④ **Post-Rec:** Keeps on recording for a set period of time after motion stops.
- ④ **Pre-Rec:** Records video for a set period of time before motion starts or an input device is triggered. This feature allows you to choose RAM or HDD as a pre-recording buffer. The difference between the two is that RAM can save smaller pre-record from 1 second to 1.5 minutes, while the hard disk can save larger one from 1 minute to 45 minutes.

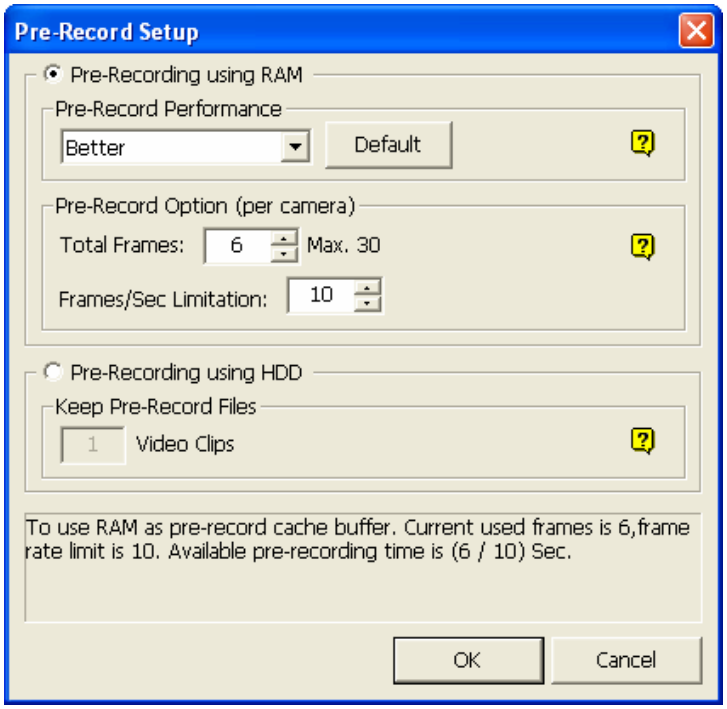


Figure 1-5

[Pre-Record Performance] The amount of physical memory of the computer that the system is running on determines the pre-recording performance. Some options are grayed out if the computer does not have enough memory for the selections.

This table shows the maximum pre-recording frame rate and the physical memory requirements of each setup:

	Good	Better	Best	Extra
Maximum pre-recording frames per camera (fps)	15 fps	30 fps	60 fps	90 fps
RAM required	128 MB	256 MB	512 MB	768 MB

Note: The recording frame rate is based on a 320x240 recording size.

[Pre-Record Option (per camera)] Determines the number of pre-record frames.

④ **Total Frames:** Specify the maximum pre-recording frames of the system.

④ **Frame/Sec Limitation:** Specify the maximum pre-recording frame rate (fps) of a camera.

Dividing the Total Frames by Frames/Sec Limitation, you will get the pre-recording duration of each camera. For example:

$$\text{Pre-recording duration} = \frac{\text{Total Frames}}{\text{Frame/Sec Limitation}} = \frac{30}{6} = 5 \text{ seconds}$$

[Pre-Recording using HDD] Use the hard disk as a pre-recording buffer. This method gives you much longer pre-recording time**.**

Keep Pre-Record Files: Specify the number of video clips for pre-record. The maximum number of video clips you can specify is 9, and the time range of one video clip is from 1 minute to 5 minutes. So the pre-recording time can be from 1 minute to 45 minutes.

④ **Use Digital Watermark Protection:** Click to watermark all recorded videos. Watermark is a way to verify the authenticity of video streams, and to ensure that they have not been tampered with or modified in any way. For details, see *Watermark Viewer* in Chapter 11.

[Video Log Storage] Select storage type (recycle or not recycle) and location. See *Setting Data Storage* later in this chapter.

1.2.2 Setting Data Storage

You can change storage locations of recorded files and event database files. You can also enable or disable the recycle function for recorded files.

Click the **Configure** button (No. 14, Figure 1-2), select **System Configure**, and select **General Setting**. In the General Setting dialog box, you can see the storage information in the middle as illustrated below.

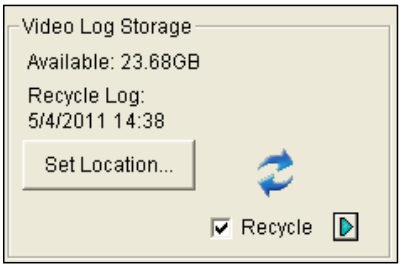


Figure 1-6

④ **Available:** Indicates the remaining hard disk space.

④ **Recycle Log:** Indicates the recording date of the next video file to be deleted.

④ **Recycle:** When this option is selected, the oldest files will be deleted when the system requires storage space for new files. If it is not selected, the system will stop recording when disk space is full.

” **Right-Arrow button:** Select the **Enlarge Recycle Threshold** option and specify the recycle threshold. Recycle threshold is the file size at which the recycling begins. The upper limit of the recycle threshold is 99999 MB.

By default, the system has the following default settings.

Default Data Storage Settings		
Storage Location	Recorded Files	:\ folder\<camxx or audxx folder>.
	Event Database Files	:\ folder\<camxx or audxx database file>
Recycle Function		Enabled

Setting the Event Database Location

The Event Database consists of the video and audio **.db** files that are used for the Video Event List. By default they are saved at the C:\ folder. Follow the steps below to change the storage location.

1. Click the **Set Location** button (Figure 1-6) and select **Database Folder**.
2. Click the **Select Files** button to specify a new storage path.

Setting the Video Storage Location

You can create the maximum of 16 storage groups with different storage locations, keep days and recycle sizes to store video files.

1. Click the **Set Location** button and select **Storage Group Folder**. This dialog box appears.

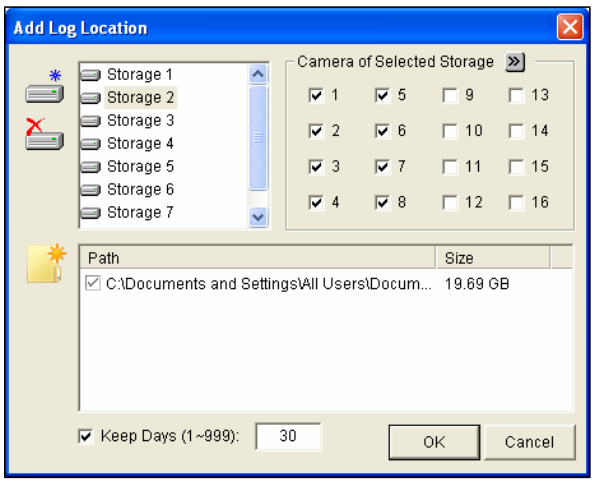


Figure 1-7

2. Click the **Add Storage Group** icon to add a storage group. The first storage group is created by default.
3. Select the cameras to be contained in the new storage group. Note one camera can only be added to one storage group.
4. Select the **Keep Days** option and specify the number of days to keep the video files in storage.
5. Click the **Add New Path** icon to specify the storage location in a hard drive which is not used for other storage groups.
6. Click **OK**.

Note:

1. If the designated storage space is not big enough to keep all video files for the defined days, the **Recycle** setting then overrides the **Keep Days** setting.
2. The video capture cards and -NVR have different default recycle thresholds. The system will delete the oldest files when the storage space reaches the following recycle threshold:

Default Recycle Threshold	
-600A / 650A / 800A	795 MB
-1120A / 1240A / 1480A / 4008	1.2 GB
-NVR	1.2 GB

Every added IP video channel can expand the default recycle threshold by 50 MB. For example, if your system of -1480A has 4 IP channels, the default recycle threshold will be 1200 MB + 50 MB x 4 = 1400 MB.

You can also use **Enlarge Recycle Threshold** to expand the threshold. Whenever the recycle threshold is reached, 400 MB of the oldest files will be deleted.

1.2.3 Adjusting Camera Configuration

In the **Camera Configure** dialog box, you can adjust the configurations for each camera. Click the **Configure** button (No.14, Figure 1-2), select **System Configure**, and click **Camera Configure** to access the following dialog box.

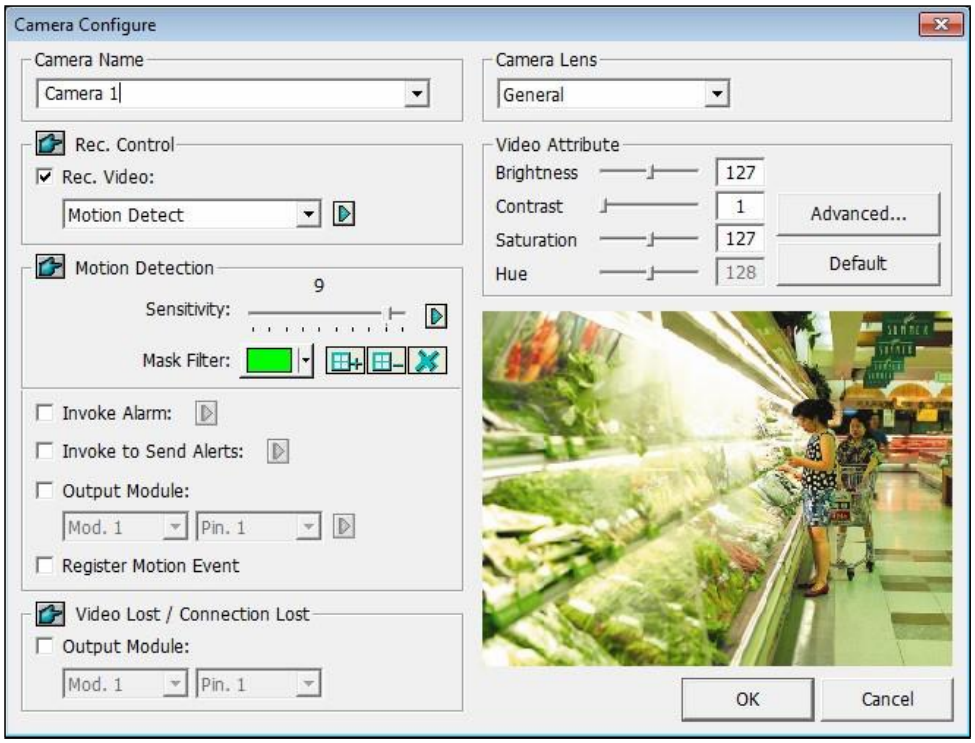


Figure 1-8 *Camera Settings*

[Camera Name] The name entered here will appear in the upper-left hand corner of the camera screen. You can use the drop-down list to select the camera to be configured.

[Rec. Control] The Rec. Control section allows you to set each camera's recording mode and frame rate. For analog cameras, you can also adjust the recording quality and resolution here.

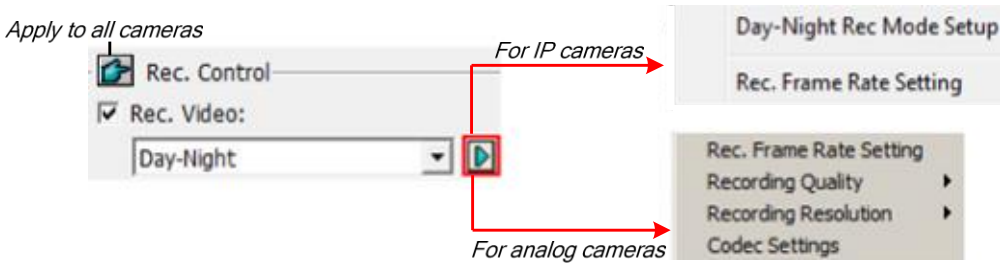


Figure 1-9

④ **Rec Video:** Enable the recording function. Use the drop-down list to select the desired recording mode: Motion Detect, Round-the-Clock or Day/Night.

④ **Right-Arrow button:** Click to set up the recording frame rate, quality, resolution, codec or Day-Night recording mode for the selected camera.

- **Day-Night Rec Mode Setup:** This option is only available when Day-Night Recording Mode is selected, allowing you to set up different recording modes during different time frames of the day. For details on Day/Night mode, see *Setting Day-Night Recording Mode* later in this chapter.
- **Rec. Frame Rate Setting:** Allows you to set the maximum recording frame so as to save storage space. For IP cameras, refer to *Economic Mode* in Chapter 2 for more details. For analog cameras, the following 4 options are available.

  - Max. recording frame rate of Non-Motion or Non-I/O Trigger: This option provides a space-saving solution for recording. Set the maximum frame rate for non-motion or non-I/O trigger periods so as to save as much storage space as possible.

  - Max. Frame Rate Rec of Motion: Set the maximum frame rate on motion detection. For example, if you set 10 Frames/sec in the field, the maximum frame this camera will record is 10 frames/second. This setting does not mean it always records at 10 frames/second because the actual recording frame rate is also affected by other settings in the system and CPU loading.

  - Max. recording frame rate of I/O Trigger: Set the maximum frame rate during I/O trigger.

  - Priority: Set **Motion First** or **I/O First** as the priority for video recording when both motion detection and I/O trigger occur at the same time. If you select **Motion First,** the frame rate setting of motion detection will override the frame rate setting of I/O trigger. If you select **I/O First,** the frame rate setting of I/O trigger will override that of motion detection.
- **Recording Quality:** Allows you to adjust the video quality of analog cameras in 5 levels. The camera's recording quality is based on its resolution and compression rate. Higher-quality picture means lower compression rate and requires more storage space. This option is only available for analog cameras.
- **Recording Resolution:** This option is only available after you change the default video resolution (see *Setting Video Source and Resolution* later in this chapter). Click to select recording resolutions. This option is only available for analog cameras.
- **Codec Settings:** Select the type of recording compression for your video. This option is only available for analog cameras.

  Geo Mpeg4: It supports a number of advanced settings that allow experienced users to adjust the encoding process. For details, see *Geo Mpeg4 Advanced Settings* later in this chapter.

  Geo H264: Provides a much smaller compressed file size than other available codec without compromising the image quality.

  Apply Advanced Codec Setting: Enable **Apply Advanced Codec Setting** and click the button. To use standard codec in recording, select **Standard Format** in the **General** tab and

the standard format of the selected recording codec will be applied. See *Geo Mpeg4 Advanced Settings* later in this chapter.

The Advanced Codec Setup button also includes the function of noise detection. See *Noise Detection to Reduce File Size* later in this chapter.

Note: To set the recording quality and codec of IP cameras, refer to *IP Channel Setup* in Chapter 2.

[Motion Detection]

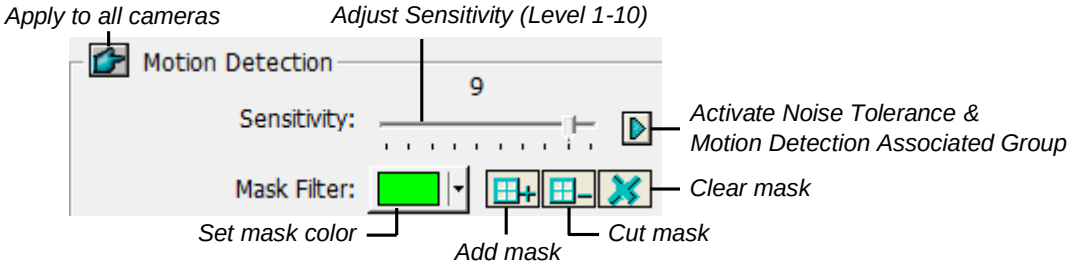


Figure 1-10

④ **Sensitivity:** There are 10 levels of sensitivity for motion detection. The default value is set to 9. The higher the value, the more sensitive the system is to the motion. Click the Arrow button to access the two options below:

- **Noise Tolerance:** This function reduces false alarms and unwanted recordings caused by weather or light changes without changing video quality. The level of noise tolerance can be adjusted. For details, see *Video Noise Solutions* later in this chapter.
- **Motion Detection Associated Group:** Refer to *Associated Monitoring* later in this chapter for more details.

④ **Mask Filter:** Mask instructs the system to ignore movement within the masked area. Mask could be applied to repetitive motion that should be ignored within the surveillance area, such as street trees.

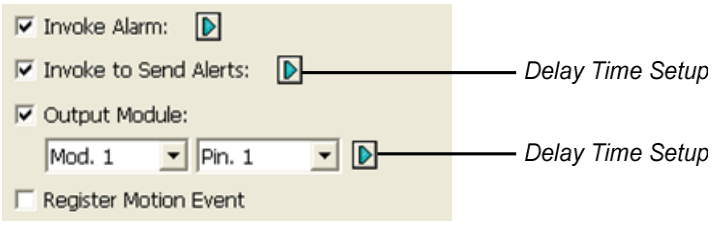


Figure 1-11

④ **Invoke Alarm:** Sends computer alarm (.wav sound file) on motion detection.

④ **Invoke to Send Alerts:** Sends an assigned alert (E-Mail/Hotline/SMS) when motion occurs. Use the drop-down list to specify the motion duration to trigger the alert. The choices include High (0.5 seconds), Normal (1 second), and Low (1.5 seconds). For example, if you choose High, the alert will be sent out when motion is detected for over 0.5 seconds.

To configure e-mail alerts, see *E-Mail Notification* later in this chapter; to configure hotline alerts, see *Hotline Notification* later in this chapter; to configure SMS alerts, see S*hort Message Service* in Chapter 10.

” **Right-Arrow button:** Sets the time to delay the activation of the assigned alerts (E-Mail/Hotline/SMS).

④ **Output Module:** Triggers the specified output module on motion detection. Use the drop-down lists to select the output module and pin number to perform this function. To configure the output device, see *I/O Device Setup* in Chapter 6.

” **Right-Arrow button:** Sets the time to delay the activation of the specified output module.

④ **Register Motion Event:** Records motion events to System Log.

Note: The Delay Time in **Invoke to Send Alerts** and **Output Module** allow you time to turn off the input device before the system triggers alerts or the output device. The Delay Time will not work if you stop monitoring or enable the function “**Deactivate notification when selected pin ON**" in I/O Application window (Figure 6-7).

[Video Lost / Connection Lost]

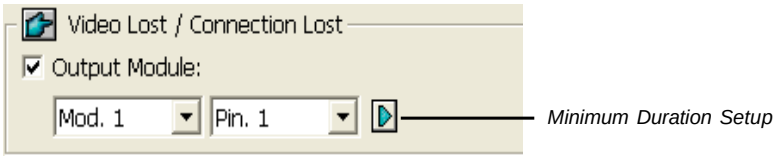


Figure 1-12

④ **Output Module:** Triggers the specified output module upon video lost or connection lost. Use the drop-down lists to select the output module and pin number to perform this function. To configure the output device, see *I/O Device Setup* in Chapter 6.

” **Right-Arrow button:** Sets the counting time between 3 and 9999 seconds for the activation of output module. If you set 30, the output module will be triggered when the video lost or connection lost lasts for 30 seconds.

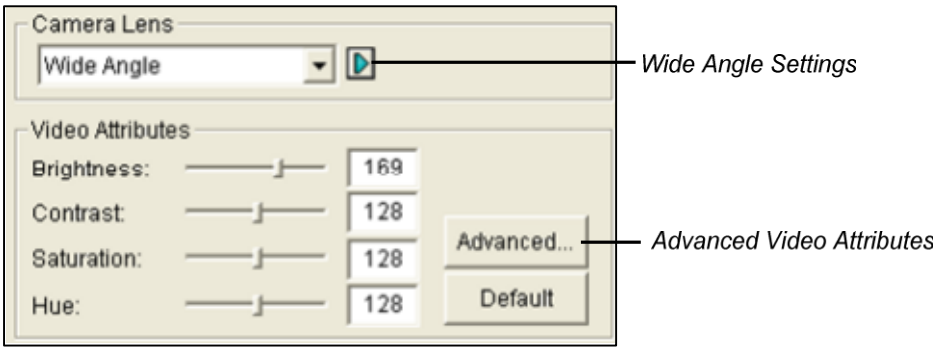


Figure 1-13

[Camera Lens] Select **Wide Angle** to correct warping toward the edge of the camera image. See *Wide Angle Lens Dewarping* in Chapter 3 for details.

[Video Attributes] Allows you to adjust video characteristics such as brightness, contrast, saturation, and hue.

[Advanced] Allows you to access the control panel of -IP cameras to adjust advanced video attributes such as white balance and shutter speed. Different image settings are available on different -IP camera models.

1.2.4 Setting Day and Night Recording Mode

Day-Night Recording allows you to set up different recording modes for different time frames of the day. Each day can be divided into 4 time frames, each represented by 1 span. You can set up a different frame rate, recording quality, motion sensitivity and noise detection level for each time frame.

1. Click the **Day-Night Recording Mode** button in Figure 1-9, and this dialog box appears.

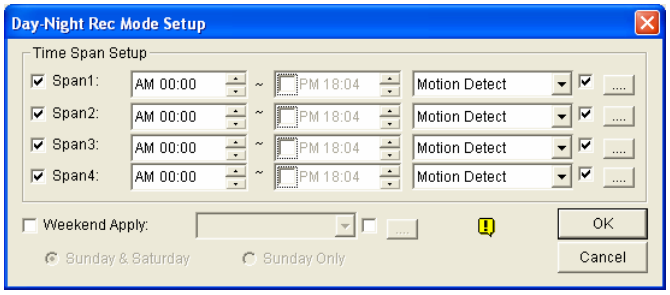


Figure 1-14

2. Enable **Span1** and specify the Start time in the first time field; select the check box in the second time field and specify the End time.
3. Use the drop-down list to select **Motion Detect** or **Round-the-Clock** to be the recording mode for the Span 1.
4. Select the check box and click the **[…]** button to adjust recording quality, motion sensitivity and noise detection level for Span 1.
5. Repeat above steps to set up multiple spans if required.
6. If you want to start monitoring all day on the weekend, select **Weekend Apply** and select recording mode to be applied. And define whether your weekend includes Sunday and Saturday or Sunday only.
7. Click **OK** to apply the settings.

Note: If the End time field is not enabled, the time span will continue to the start of the next span.

1.2.5 Geo Mpeg4 Advanced Settings

The Geo Mpeg4 codec supports a number of advanced settings that allow experienced users to adjust the encoding process.

In Figure 1-9, check the **Apply Advanced Codec Setting** option, click the button beside, and then click the **Advanced** tab. This window appears.

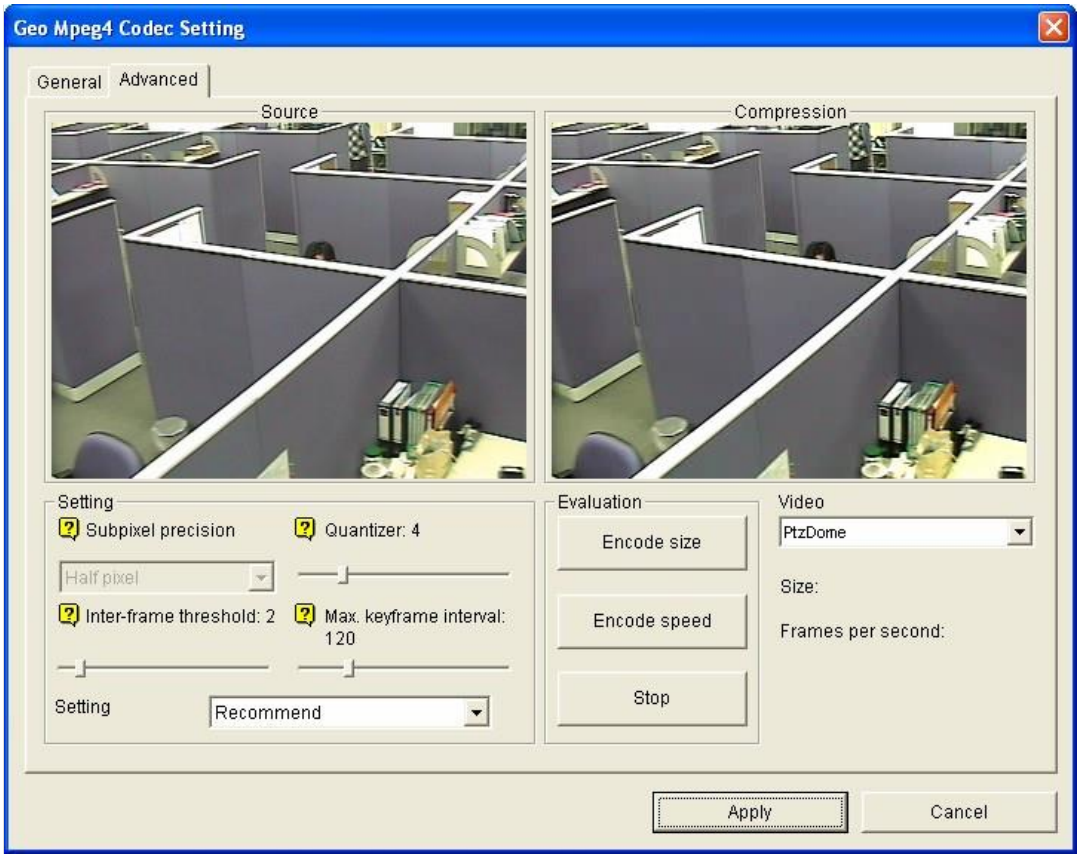


Figure 1-15

[Setting]

④ **Setting:** Click the drop-down list to select **High speed**, **Recommend**, or **High compression rate** for default configurations. Or, select **User-defined** to define encoding settings yourself.

④ **Subpixel precision:** Click the drop-down list to select Full, Half or Quarter pixel.

Full pixel: Fastest compression speed, medium compression rate, and normal image quality.

Half pixel: Fast compression speed, high compression rate, and better image quality. **Quarter pixel:** Slow compression speed, highest compression rate, and better image quality.

④ **Quantizer:** Raising the value will improve compression speed and dramatically increase compression rate, but reduce image quality.

④ **Inter-frame threshold:** Raising the value will improve compression speed and rate, but reduce image quality slightly.

④ **Max. key frame interval:** Raising the value will extend the duration between key frames and increase compression rate, but reduce image quality slightly. Compression speed remains the same.

[Evaluation]

④ **Encode size:** Click to calculate the encoding size based on your encoding settings (see *[Setting]* above) and assigned video clip (select **PTZ dome** or **street** from the drop-down list). Click the **Stop** tab to stop the evaluation.

④ **Encode speed:** Click to calculate the frame rate based on the encoding settings (see *[Setting]* above) and assigned video clip (select **PTZ dome** or **street** from the drop-down list).

1.2.6 Customizing Startup Settings

The Startup dialog box allows you to set the system to enable selected features at system startup. To access the Startup dialog box, click the **Configure** button (No.14, Figure 1-2), select **System Configure** and click **Startup**.

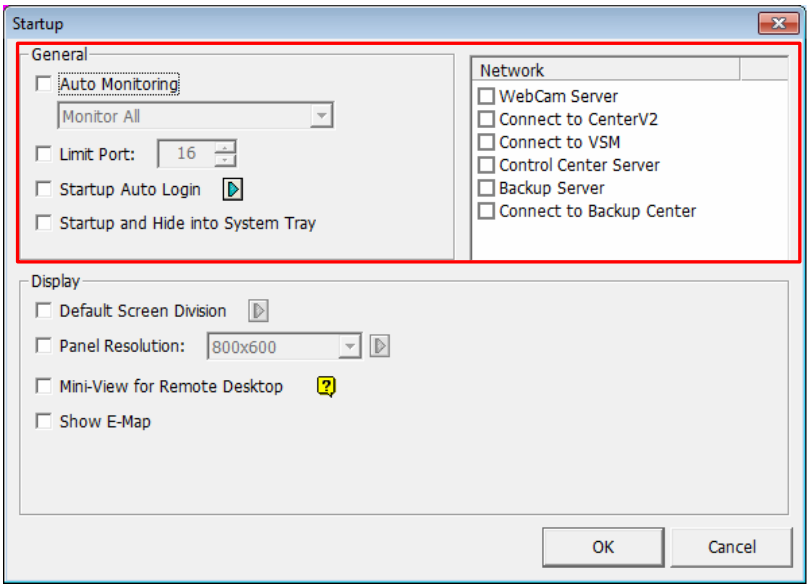


Figure 1-16

[General]

④ **Auto Monitoring:** Select one of the following monitor control modes at system startup:

- **Monitor All:** Allows you to monitor all cameras and I/O (if available) at system startup. It is the same as to manually click **Monitor** button (No. 16, Figure 1-2) and select **Start All Monitoring**. (For details, see *Camera Monitoring* later in this chapter).
- **Schedule Monitor:** Allows you to monitor cameras by schedule. Alternatively you may click **Schedule** button (No. 15, Figure 1-2) and select **Schedule Start**. Refer to *Recording Schedule* later in this chapter.
- **I/O Monitor:** Allows you to monitor all I/O devices. Alternatively you may click the **Monitor** button (No. 16, Figure 1-2), and then select **I/O Monitoring**.
- **Camera Monitor:** Enables all cameras for monitoring.

Note: To set different recording modes and alert methods for each camera, see *Monitor Control* in *Adjusting Individual Camera* later in this chapter.

---

④ **Limit Port:** Limits the number of video ports to be used. This option helps increase the frame rate of each channel by shifting the frame rate of disabled video ports to enabled ones. This function will take effect at next system startup.

④ **Startup Auto Login:** Select and press the **Arrow** button to assign an ID used at system auto startup. After the setup, the system will automatically login using this ID at next startup, without asking for ID and Password.

④ **Startup and Hide into System Tray:** -System appears in the system tray when you launch Windows instead of displaying the system login window.

[Network]

④ **WebCam Server:** Allows connection to WebCam Server at system startup. (Or click the **Network** button (No. 11, Figure 1-2) and select **WebCam Server**.)

④ **Connect to Center V2:** Allows connection to Center V2 at system startup. (Or click the **Network** button (No. 11, Figure 1-2) and select **Connect to Center V2**.)

④ **Connect to VSM:** Allows connection to VSM Server at system startup (Or click the **Network** button (No. 11, Figure 1-2) and select **Connect to VSM**.)

④ **Control Center Server:** Allows connection to Control Center Server at system startup. (Or click the **Network** button (No. 11, Figure 1-2), select **Control Center Server** and select **Control Center Service**.)

④ **Backup Server:** Allows connection to Backup Server at system startup. (Or click the **Network** button (No. 11, Figure 1-2) and select **Backup Server**.)

④ **Connect to Backup Center:** Allows connection to Backup Center at system startup. (Or click the **Network** button (No. 11, Figure 1-2) and select **Backup Center**.)

1.2.7 Customizing Display Settings

You can customize the display settings in the Display section of the Startup dialog box. Click the **Configure** button (No.14, Figure 1-2), select **System Configure** and click **Startup**.

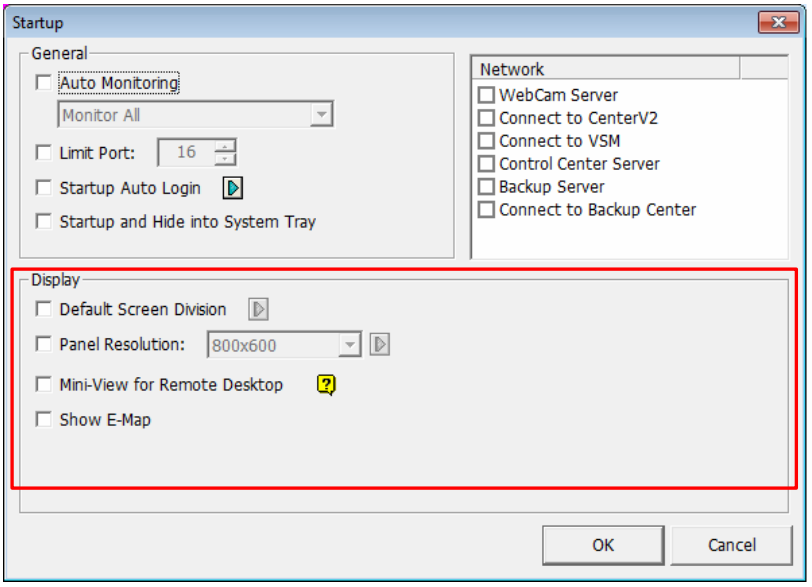


Figure 1-17

④ **Default Screen Division:** Select the number of screen division to display at startup.

④ **Panel Resolution:**

” From the drop-down list, select the resolution that best fits your computer monitor screen. For the monitor display ratio supported by each panel resolution, see *Appendix H*.

” Click the **Arrow** button and select **Activate Quad Enhanced** to enable the enhanced screen layout for the 8, 12 and 16 screen divisions. The layout 1 is the default layout; the layout 2 is the enhanced layout.

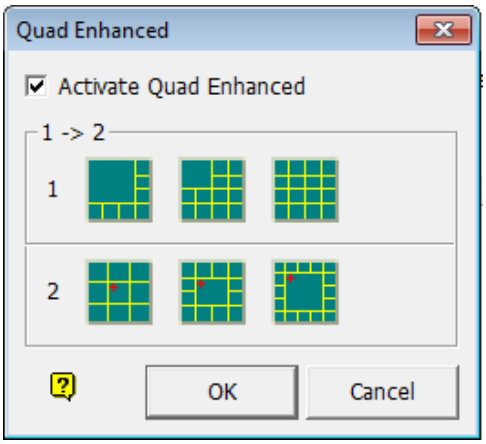


Figure 1-18

Note:

1. When the enhanced screen layout is applied, camera 1 view will be displayed in the central screen. When the popup feature is enabled, the pop-up view will show on the central. When the camera scan feature is enabled, the scanned view will show on the central.
2. The enhanced screen layout cannot be applied when DSP card is in use.
3. The enhanced screen layout will be applied at next startup.

④ **Mini-View for Remote Desktop:** Squeezes all video channels into a single 320x240 view. Since you may use Microsoft Remote Desktop (a feature that comes with Windows XP Professional Edition) to set up the Main System through network, it is important to get smallest size possible data to transfer over network.

After Mini-View for Remote Desktop is selected, restart the Main System and you can now switch between the mini and normal view by clicking the **Configure** button (No.14, Figure 1-2), pointing to **A/V Setting** and selecting **Mini-View Switch**.

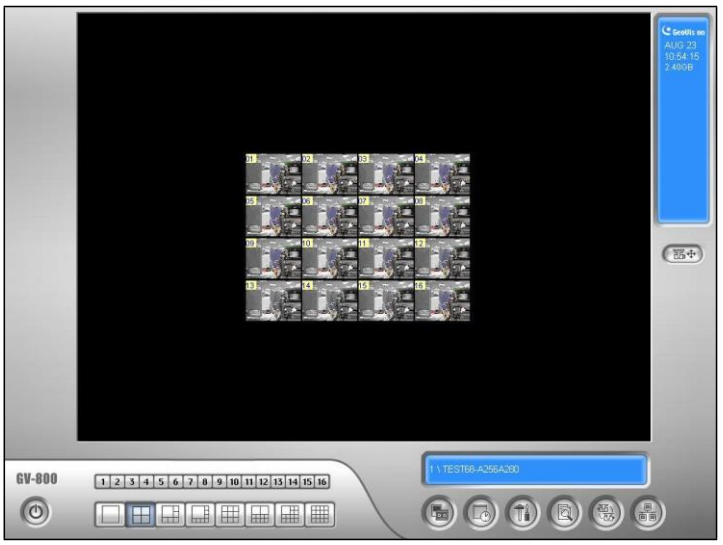


Figure 1-19 Mini View

④ **Show E-Map:** Displays the setup E-Map Viewer window (Figure 9-5) at system startup.

1.2.8 Setting Auto Reboot

The Auto Reboot feature restarts -System and Windows at a scheduled time. Click the **Configure** button (No.14, Figure 1-2), select **System Configure**, and select **Auto Reboot Setup**.

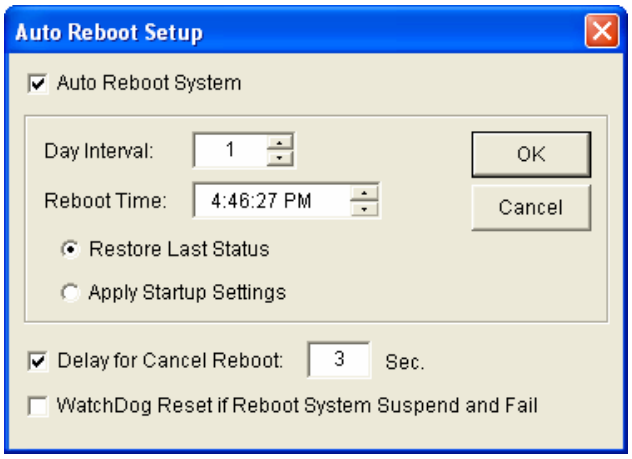


Figure 1-20

[Auto Reboot System] Enables the automatic reboot of the -System and Windows.

④ **Day Interval:** Specifies the frequency of auto reboot (from 1 to 14 days). After the Day Interval is modified, the new day interval will start counting from the last reboot date instead of the day when the change is applied, unless you restart the -System.

④ **Reboot Time:** Specifies the reboot time.

- **Restore Last Status:** The system will resume the last operation after rebooting, e.g. camera recording.
- **Apply Startup Settings:** The system will apply your Startup settings in System Configure section after rebooting.

[Delay for Cancel Reboot] When the item is checked, a warning message will appear and count down for the specified seconds before the reboot schedule begins. Clicking the **Cancel** button on the prompt will cancel the rebooting.

[Watchdog Reset if Reboot System Suspend and Fail] Prior to the Reboot Time, if -System finds any abnormal Windows operation that may hinder the Auto Reboot, -System will instruct a hard reboot on the computer. The feature is not available in -250 Card and -NVR System.

Note: -System must already be added to Windows Startup menu; only so will the Windows automatically restart -System after a reboot. Also, make sure you've correctly connected a video capture card to your motherboard for the hardware watchdog feature.

1.2.9 Setting Text Overlay

You can align camera name, time stamp and triggered input name to different positions for each channel.

To access this feature, click the **Configure** button (No.14, Figure 1-2), select **System Configure**, and select **Text Overlay Setting** to display the Text Overlay Setting dialog box, and select one **Camera** to be defined.

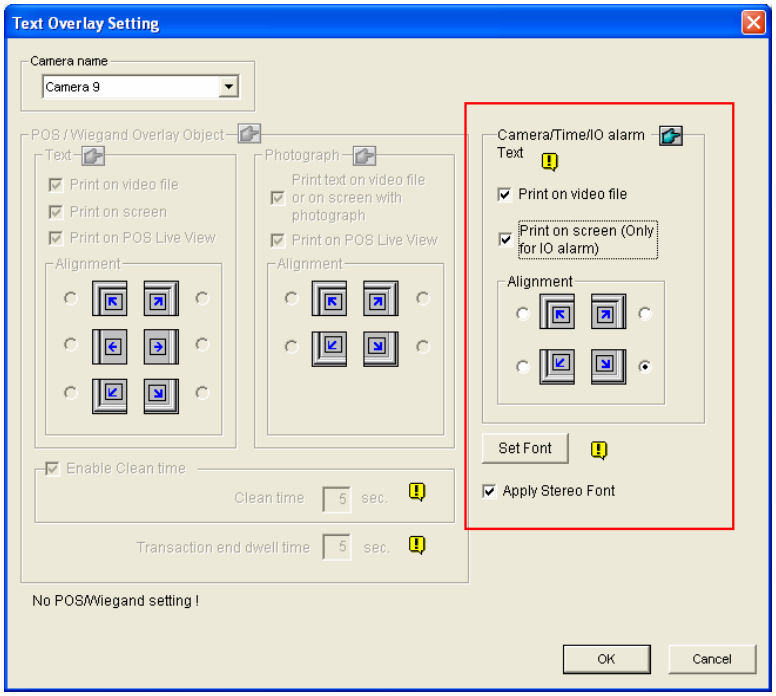


Figure 1-21

[Camera/Time/IO Alarm Text]

④ **Print on video file:** Displays camera ID, location name, date and time on the recorded video.

Note: Text overlay is not supported when standard format codec is enabled.

---

④ **Print on screen (Only for IO alarm):** Displays the name of triggered input device on the camera screen. For this function to work, it is required to map a camera to an input device, see *Overlaying Input Device Name onto Screen upon Input Trigger* in Chapter 6.

Note: Up to 5 input names can be stamped on each channel when inputs are triggered.

---

④ **Alignment:** Select how you want the camera information to be aligned on a camera screen.

[Set Font] Click the **Set Font** button to set up the font. The option **Apply Stereo Font** makes texts stand out from the background by giving white-edge to the texts.

1.3 Audio and Video Settings

1.3.1 Setting Video Source and Resolution

Video Source sets the video standard of your system: NTSC or PAL. Click the **Configure** button (No.14, Figure 1-2), select **A/V Setting**, and select **Video Source** to display the following dialog box.

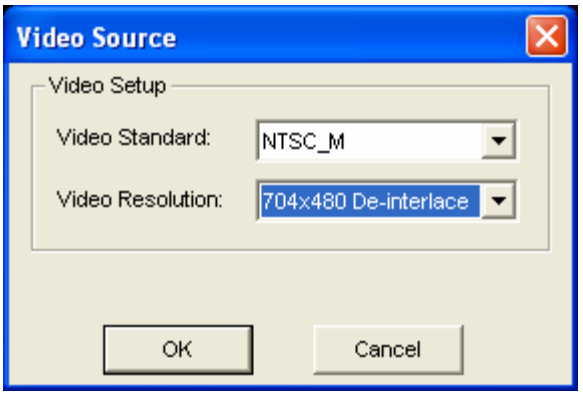


Figure 1-22

④ **Video Standard:** Select a video standard used in your country.

④ **Video Resolution:** Consider your priority in image quality or CPU usage before making a selection.

⌘ For NTSC, the image quality and CPU usage from the highest to the lowest is: 704 x 480, 704 x 480 De-interlace, 640 x 480, 640 x 480 De-interlace, 352 x 240, 320 x 240.

⌘ For PAL, the image quality and CPU usage from the highest to the lowest is: 704 x 576, 704 x 576 De-interlace, 640 x 480, 640 x 480 De-interlace, 352 x 288, 320 x 240.

To change the resolution of individual analog cameras, refer to *Resolution Button* in *Adjusting Individual Camera* earlier in this chapter.

1.3.2 Fixing Aspect Ratio

This feature lets you define your own aspect ratio for the camera channels so they will not be stretched when viewed in wide screen resolutions such as 1280 x 800, 1440 x 900, 1680 x 1050 and 1920 x 1080.

Click the **Configure** button (No.14, Figure 1-2), select **A/V Setting**, and select **Wide Display Setup**. This dialog box appears.

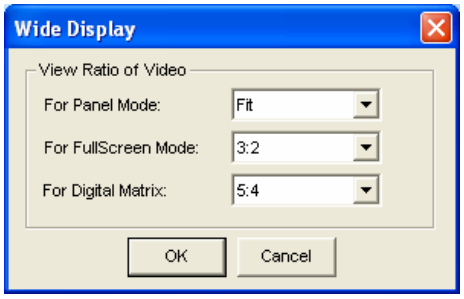


Figure 1-23

④ **Fit:** Automatically fits the video ratio into the camera channel. The outcome will be stretched in wide screen resolution.

④ **3:2:** Changes the aspect ratio of the camera channel to 3:2.

④ **4:3:** Changes the aspect ratio of the camera channel to 4:3.

④ **5:4:** Changes the aspect ratio of the camera channel to 5:4

For Digital Matrix, see *Chapter 11 Useful Utilities*.

1.3.3 Adjusting Video Attributes

This feature lets you adjust video attributes to get the best picture. Click the **Configure** button (No.14, Figure 1-2), point to **A/V Setting**, and select **Video Attributes** to choose between **Standard** and **Advanced**.

Users of -Combo A Card (-1016/ -1120A/1240A/1480A), -600A, -650A and -800A can also select **Default Value** to change the default video attributes to **Vivid** or **Standard**. The **Vivid** option produces more saturated and colorful video images, while the **Standard** option produces brighter and less saturated video images. You must click the **Default** button in Standard Video Attributes or Advanced Video Attributes to apply the selected default values.

Note: The Video Attributes feature is only available for analog cameras.

Standard Video Attributes

Adjust image quality by moving the sliders to the desired values. Click **Default** to apply default values. Click the **left** and **right arrow** buttons to select a desired camera for setup. Or, click the **finger** button to apply the displayed settings to all cameras.

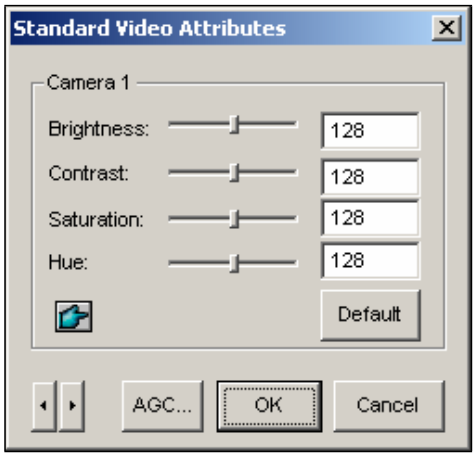


Figure 1-24

AGC (Auto Gain Control): This option is only available on -600A, -650A and -800A. Adjusting AGC helps boost weak video signals or reduce strong video signals, and gives optimized image quality. The adjustment could be done manually or automatically. When a video signal is weak, for example, due to distance, adjusting the brightness or contrast of the video source will NOT help the situation. Adjust AGC and see the difference.

In the Auto Gain Control window, click **Auto** for auto adjustment, click **Default** to apply default values, or click **Apply** to apply the displayed settings. The default value is set to 1.15V (115), but you may move the slider to adjust between 0.3V (30) or 2.5V (250).

Advanced Video Attributes

In addition to adjust standard video attributes, you can adjust image quality and codec. With the advanced settings, you can even see the difference in image size after you have these adjustments.

[Multicam]

This feature helps you to see the difference in image size after you adjust video attributes, codec and recording quality. Your selection here will also be applied to the assigned camera.

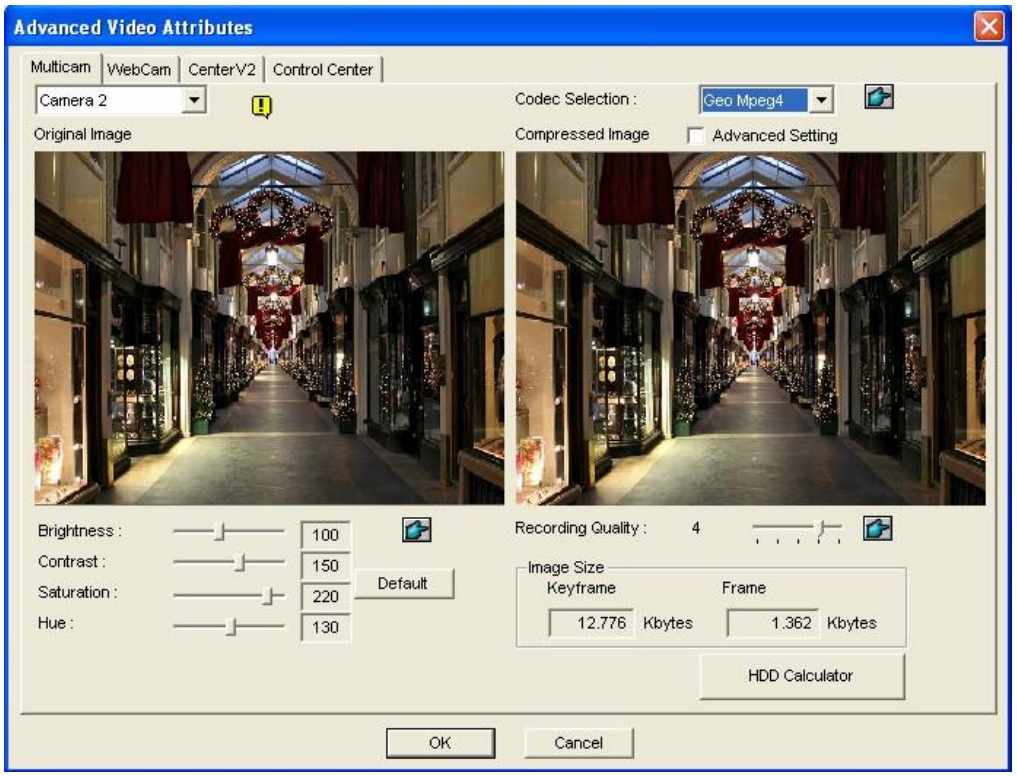


Figure 1-25

④ **Camera drop-down list:** Select a camera channel for the application.

④ **Codec Selection:** Select a desired type of compression.

④ **Image Adjustment (Brightness, Contrast, Saturation, Hue):** Move the sliders to adjust image attributes. Click the finger button to apply the selected values to all cameras.

④ **Recording Quality:** Move the slider to increase or decrease the picture quality. Click the **finger** button to apply the selected quality to all cameras.

④ **Image Size: Keyframe** indicates the compressed file size while **Frame** shows the partly compressed file size after quality and image adjustment.

Note: The smaller image size means higher video compression and smaller file size, thus extending the recording capacity.

[WebCam, Center V2, Control Center]

You can configure the image quality for video streaming to the WebCam server, Center V2 and Control Center. Your quality settings for Low, Normal and Best will be applied to these remote applications.

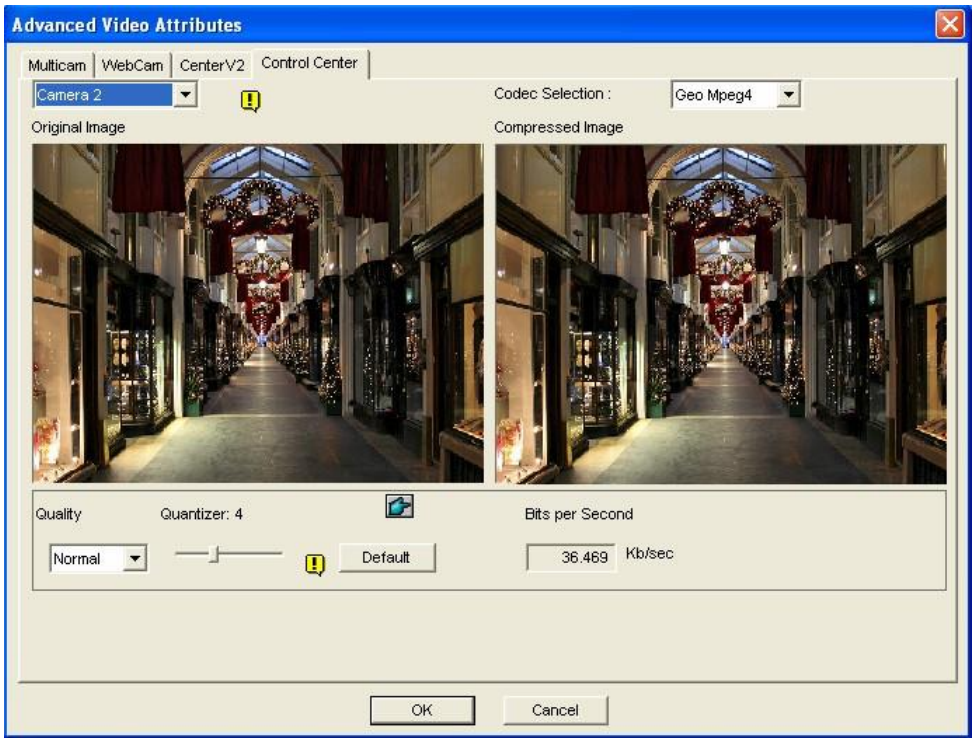


Figure 1-26

④ **Quantizer:** The bigger the Quantizer, the poor the image quality.

④ **Quality:** The default Quantizer for Best is 2, for Normal is 4 and for Low is 8. The adjustment rule between Quantizer and Quality is: Quantizer for Best < Quantizer for Normal < Quantizer for Low.

④ **Bits per second:** Indicates the data transmission speed after quality adjustment.

④ **Codec Selection:** The codec selection is for your reference only to know the bitrate. The selection will not be applied to video streaming to the remote applications.

1.3.4 Adjusting Audio Setting

You can adjust audio devices to record and listens to live sound. Click the **Configure** button (No.14, Figure 1-2), select **A/V Setting**, and select **Audio Settings** to bring up the following dialog box:

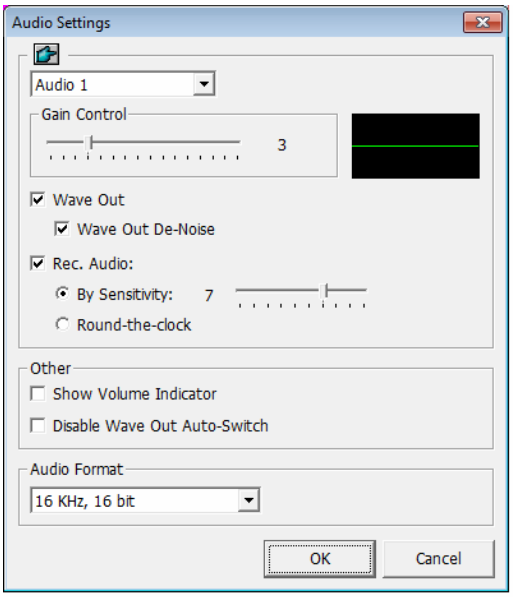


Figure 1-27

[Audio]

④ **Audio:** Select an audio channel to be configured. Clicking the **finger** button can apply the settings of one audio channel to the rest of channels.

④ **Gain Control:** Increases or decreases the gain of the microphone.

④ **Wave Out:** Listens to the audio around the camera.

” **Wave Out De-Noise:** Reduces audio noise.

④ **Rec Audio:** Activates the audio recording.

” **By Sensitivity:** Audio recording is activated when the volume reaches the sensitivity level indicated.

” **Round-the-Clock:** Continuously records audio.

[Other]

④ **Show Audio Indicator:** Displays an audio volume indicator in the top-left corner of the camera view.

④ **Disable Wave Out Auto-Switch:** By default, audio channel 1 is set to be background sounds even when you switch between video channels. To change background sounds, select the desired audio channel and select **Disable Wave-Out Audio Switch**. The selected audio channel will always be in the background.

[Audio Format]

- **16kHz, 16 bit:** By default, -System is set to this audio codec.
- **32kHz, 16 bit:** Select this audio codec for better audio quality if you are using -5016 / 4008 / 4008A / 900A / 8008 / 6508 / 6008 / 1480A / 1240A / 1120A / 14808 / 12408 / 11208 Card.

1.3.5 Turbo Mode

Turbo mode allows recording at the highest speed that **-Combo A Card** (-1120A, -1240A and -1480A) can provide at the VGA and D1 resolutions.

Comparison for -Combo Card and -Combo A Card

	Total Recording Rate (NTSC/PAL)					
	-1480	**-1480A**	**-1240**	**-1240A**	**-1120**	**-1120A**
VGA	120 / 100 fps	240 / 200 fps	120 / 100 fps	120 / 100 fps	80 / 70 fps	80 / 72 fps
D1	120 / 100 fps	240 / 200 fps	120 / 100 fps	120 /100 fps	80 / 70 fps	80 / 72 fps
Turbo VGA		**416 / 400 fps**		**240 / 200 fps**		**120 / 100 fps**
Turbo D1		**352 / 320 fps**		**240 / 200 fps**		**120 / 100 fps**

Note: When Turbo Mode is activated, the DSP (Real-Time Display) and TV-Out functions will be disabled.

System Requirements

Following is the basic system requirements to activate the turbo mode.

Video Capture Card	CPU	RAM	Graphic Card	HDD
-1120A x 1	Pentium 4, 3.0 GHz, Dual Core	2 x 512 MB Dual Channels (Windows XP) 2 x 1 GB Dual Channels (Windows Vista / 7 / 8 / Server 2008 / 2012)	AGP or PCI-Express, minimum 800 x 600 (1280 x 1024 recommended), 32-bit color	120 GB
-1240A x 1	Core 2 Duo, 3.0 GHz			160 GB
-1480A x 1	Core 2 Quad, 2.4 GHz			320 GB
-1120A x 2	Core 2 Quad, 2.4 GHz	2 x 1 GB Dual Channels		250 GB
-1240A x 2	Core 2 Quad, 2.8 GHz			320 GB
-1480A x 2	Core i7-920, 2.66 GHz			750 GB

Activating Turbo Mode

1. Click the **Configure** button (No. 14, Figure 1-2), select **A/V Setting** and select **Video Source**. This dialog box appears.

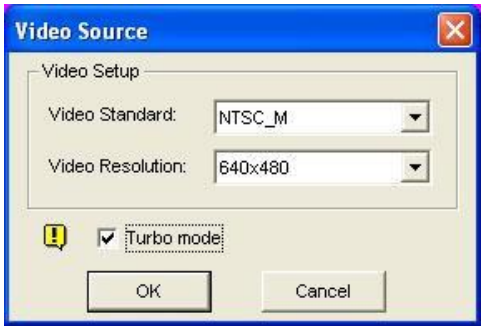


Figure 1-28

2. Use the drop-down list to select the Video Resolution. If D1 or VGA resolution is selected, the **Turbo mode** option appears.
3. Select **Turbo mode**, and click **OK**.
4. You will be prompted to restart -System. Restart the -System to take effect.

1.4 Camera Monitoring

Click the **Monitor** button and select to start or stop all or individual camera monitoring. Camera Name in the upper left corner of the view screen changes from yellow to red color when motion is detected. (Blinking represents that motion is detected in the camera view). **[F7]** is the shortcut key of this operation.

1.4.1 Snapshot

To take a snapshot of the current frame, click the Camera Name and select **SnapShot** to open the Save As dialog box, shown as below. You can select to watermark or de-interlace the snapshot, as well as tagging the frame with Host name, Camera name, Time and Date. Select **Transparent Text** if you want to make the tag background transparent, and select **Set Font** to choose your text font.

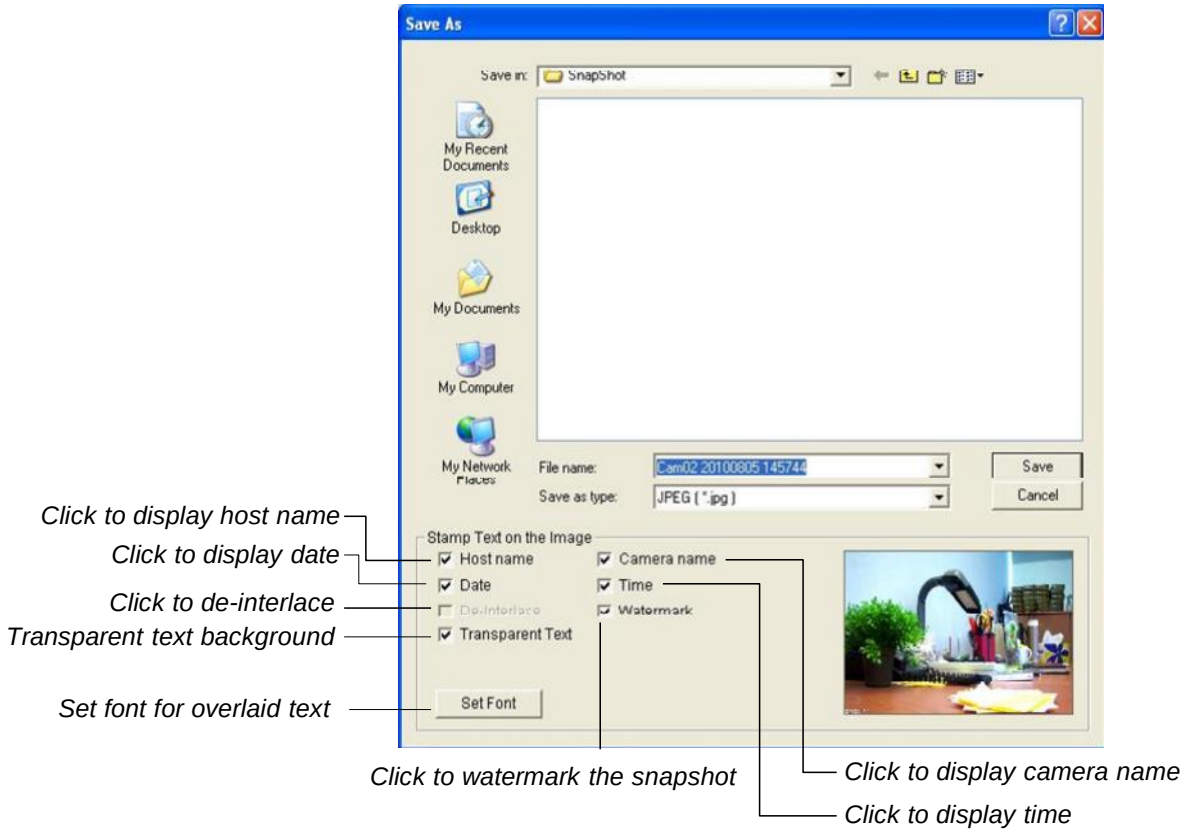


Figure 1-29

1.4.2 Associate Monitoring

You can set camera channels to start recording when any of the associated camera channels begins recording.

1. Click the **Configure** button (No. 14, Figure 1-2), select **System Configure**, and select **Camera Configure**. This dialog box appears.

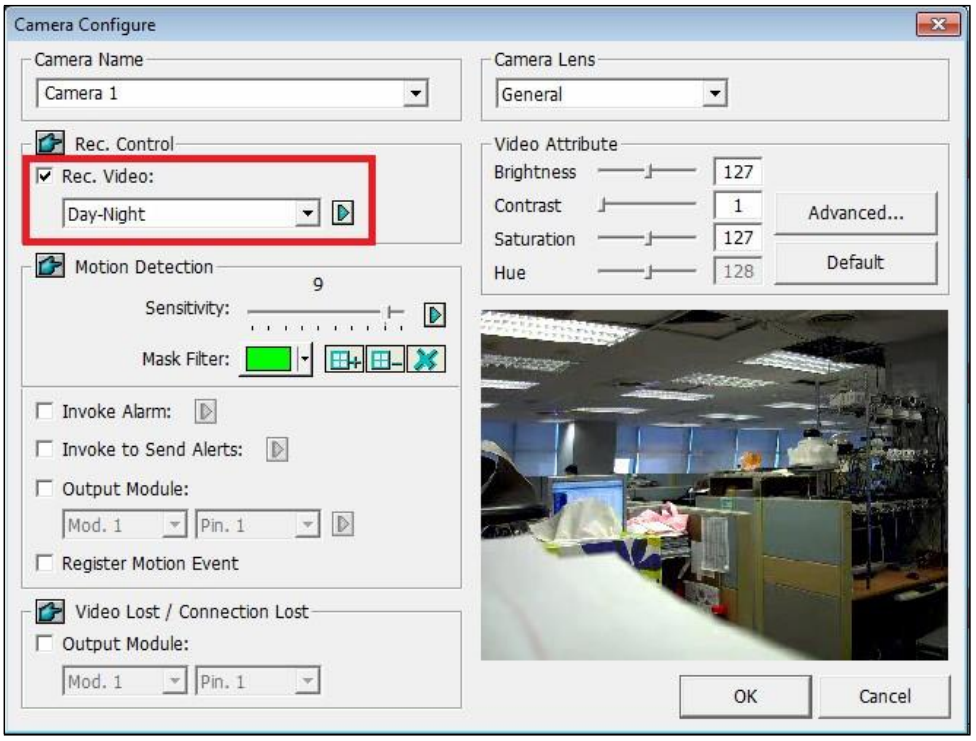


Figure 1-30

2. From the **Rec. Video** drop-down list, select either **Motion Detect** or **Day-Night**. If you select **Day-Night**, remember to click the **Arrow** button beside to configure the time spans and also set the recording mode to be **Motion Detect**.
3. Click the **Arrow** button on the right of **Sensitivity**, and select **Motion Detection Associated Group**. This dialog box appears.

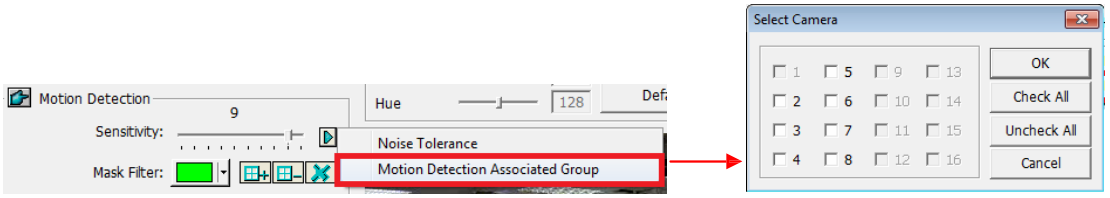


Figure 1-31

4. Select the camera channels you wish to be associated with the current camera. In this example, Camera 1 is being configured and it cannot be selected, so it is grayed out. Cameras 2 and 3 are selected to be associated with Camera 1.
5. Click **OK** to apply the settings.

From the example (Figure 1-31), whenever Camera 2 or 3 starts recording, Camera 1 will also begin recording.

1.4.3 Daylight Saving Time Recording

The -System can automatically adjust to Daylight Saving Time (DST).

To enable the DST function, click Windows **Start** button, click **Control Panel**, click **Date and Time**, click the **Time Zone** tab, select a time zone of your location, and then select **Automatically adjust clock for daylight saving changes**.

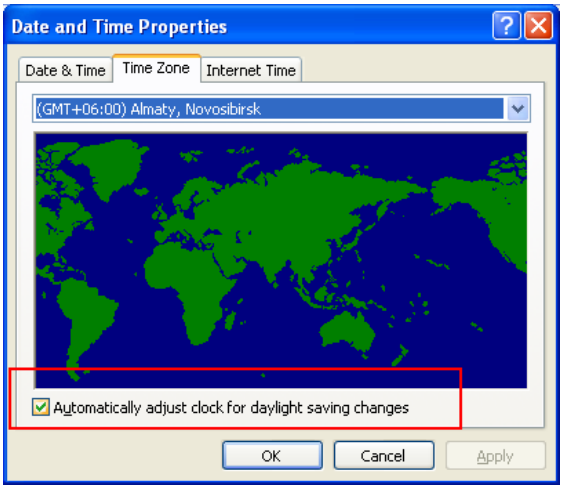


Figure 1-32

In System Log, the DST recordings can be identified in the **D.S.T Rollback** column.

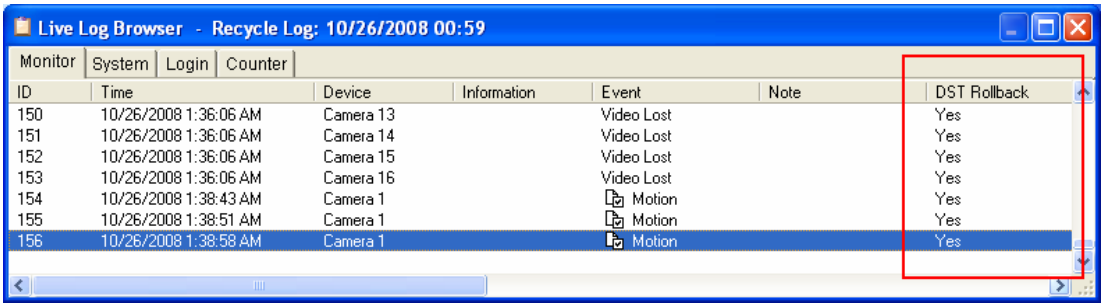

Live Log Browser - Recycle Log: 10/26/2008 00:59
Monitor
System
Login
Counter
ID Time Device Information Event Note DST Rollback
150 10/26/2008 1:36:06 AM Camera 13 Video Lost Yes
151 10/26/2008 1:36:06 AM Camera 14 Video Lost Yes
152 10/26/2008 1:36:06 AM Camera 15 Video Lost Yes
153 10/26/2008 1:36:06 AM Camera 16 Video Lost Yes
154 10/26/2008 1:38:43 AM Camera 1 Motion Yes
155 10/26/2008 1:38:51 AM Camera 1 Motion Yes
156 10/26/2008 1:38:58 AM Camera 1 Motion Yes

Figure 1-33

In ViewLog, a separate DST subfolder will be displayed in the Date Tree.

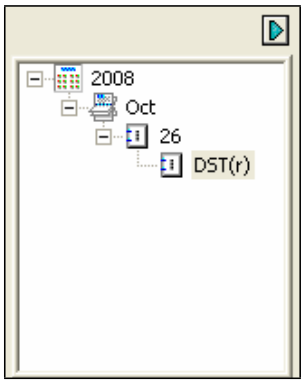


Figure 1-34

Note: The AVI file recorded during the DST period is named with the prefix " DST", e.g. DST20081022xxxxxxxxx.avi, to differentiate from the regular AVI file named with the prefix "Event", e.g. Event20081022xxxxxxxxx.avi.

1.5 Account and Password

The password setup allows you to assign permission and rights to users. You can create up to **1,000** passwords. The system will control and restrict access to system resources based on the permission and rights associated with each user account. Only Supervisor account level is pre-set with access to the Password Setup function. Click the **Configure** button (No. 14, Figure 1-2), point to **System Configure**, point to **Password Setup**, and then select **Local Account Edit** to display the following window.

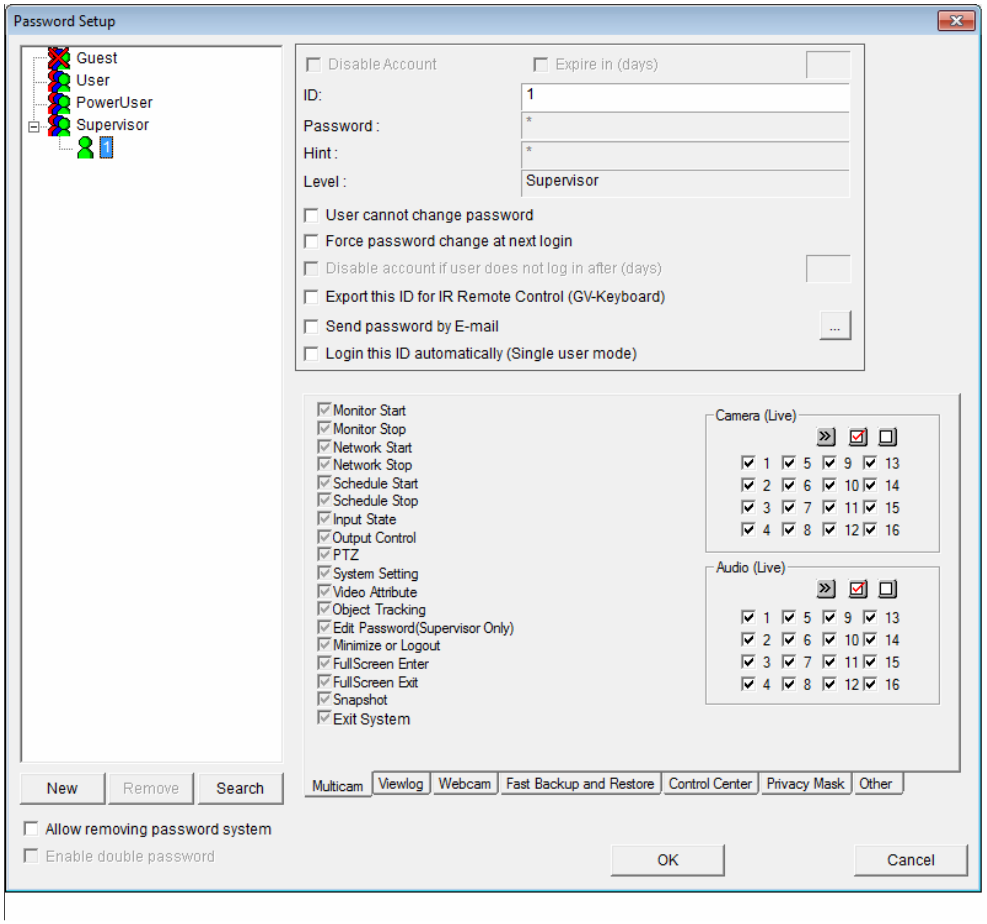


Figure 1-35

1.5.1 Creating an User Account

To create a user account:

1. Click the **New** button at the lower-left hand corner to bring up the New Account dialog box.

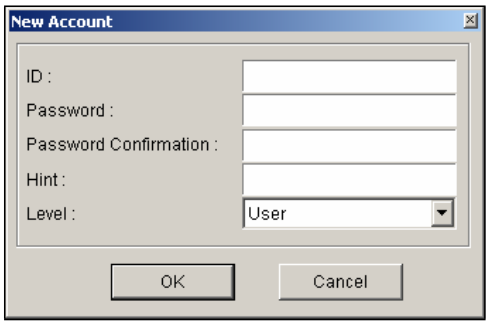


Figure 1-36

2. Enter the user's **ID** name and **password**. Re-enter the same password in the Password Confirmation field.
3. Give a **Hint** (optional) that would remind you of the password.
4. Select the user's authorization level: **Supervisor**, **PowerUser** or **User**. By default, users belonging to the Supervisor level have full rights over -System settings. PowerUsers have the same permission and rights as Supervisors, except that they cannot edit user information and delete the password system (described later). Users belonging to the User level are restricted to all system settings, and have only limited access to certain functions. Click **OK** to add the user.
5. If you want to enable the guest account, click **Guest** and clear the selection for **Account is disabled**. Guests are only allowed to view videos.

To edit an exiting user account:

This feature is only available for supervisors.

1. Select a user from the user list to display its properties. Or, right-click on any of the user levels (User, PowerUser, Supervisor), and then select **Find Specific Account** for quick search. A valid password is required to edit a supervisor.
2. Edit the properties as required. Check the **Account Is Disabled** option if you wish to disable this user.

You may also find these options in the dialog box:

④ **Expire in xx day(s):** The account will expire and be disabled automatically after a set number of days. The number you set will count down automatically. Specify the number between 1 and 9999.

④ **User cannot change password:** The user is not allowed to change the set password.

④ **Force Password change at the first logon:** The user must change the password when logging in first time.

④ **Disable user if do not login after xx day (s):** When the user does not log in the system after a set number of days, its account will be disabled automatically.

④ **Export this ID for IR Remote Control:** Allows you to log into the system by using the -Keyboard instead of using the general keyboard and mouse. For details see *-Keyboard User's Manual*.

④ **Send Password by Email**: Allows you to retrieve passwords through e-mails. To specify e-mails, click the **[…]** button. For details on this feature, see *Retrieving Password Through E-mail* later in this chapter.

④ **Allow removing password System:** Enables the password removal utility. The option is critical if you forget or unable to retrieve any Supervisor password in the future. With this option selected, you can run the password removal utility ***PassUNINStall.exe*** from the folder and remove the password database. Otherwise, you can only remove the password database by reinstalling Windows operating system.

Note:

The loss of passwords can be solved in the following two ways:

1. Retrieving password through e-mails.
2. Removing password database by using the *PassUNINStall.exe* utility and rebuilding all accounts.

However, if both **Send Password by Email** and **Allow Removing Password System** options are not selected in advance, it is required to reinstall Windows operating system once you loss the passwords.

1.5.2 Changing Password on Login

1. When you log in the -System, click the **Change Password** button in the Login dialog box. The Change Password dialog box appears.

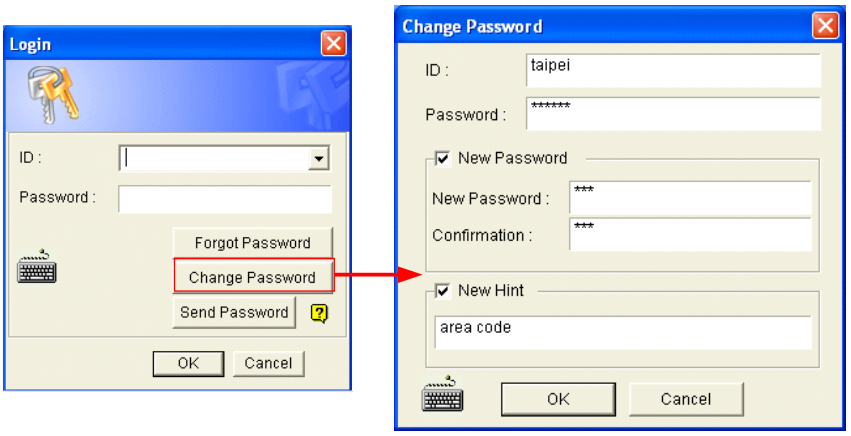


Figure 1-37

2. Type the new password information, and click **OK** to save the changes.

Note: Only Supervisors can change the password.

1.5.3 Retrieving Password Through E-mail

The password retrieval function can serve in the following ways after you click the **Send Password** button at the Login window (Figure 1-37):

- If you are one of supervisors but do not remember your ID, separate passwords will be sent to all supervisor e-mail accounts after you click the **Send Password** button.
- If you are one of the supervisors and remember your ID but forgot your password, enter your ID and then click the **Send Password** button. The password will be sent to your e-mail account.
- If you are not a supervisor, enter your ID and then click the **Send Password** button. The e-mail with your password will be sent to you.

1.5.4 Preventing Unauthorized System Termination

The -System can be protected from stopping or restarting by an unauthorized user. To restrict a user who does not belong to the **Supervisor** level from existing or restarting the system, follow the steps below:

1. Click the **Configure** button (No. 14, Figure 1-2), select **System Configure**, select **Password Setup**, and select **Local Account Edit**. The Password Setup dialog box appears.
2. Select a user from the user list to display its properties.
3. Select the **Multicam** tab at the bottom, and clear the **Exit System** option to restrict the user from quitting or restarting the system.

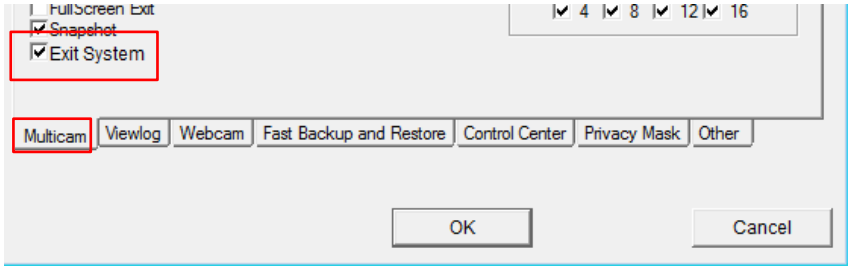


Figure 1-38

1.5.5 Setting Double Passwords for ViewLog Access

You can select the **Enable Double Password** option to require two supervisor passwords to access the ViewLog and play back recorded files. The option is only available when you have created at least two supervisor accounts. For details on the ViewLog, see Chapter 4.

1. Click the **Configure** button (No. 14, Figure 1-2), select **System Configure**, select **Password Setup**, and select **Local Account Edit**. The Password Setup dialog box appears.
2. Select **Enable Double Password** at the bottom.

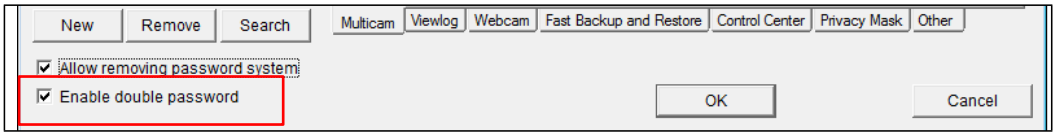


Figure 1-39

After clicking the **ViewLog** button, you will need to type the passwords of any two supervisors to be able to login.

1.6 System Idle Protection

The System Idle Protection allows the administrator to work on the system without the worry of logout or leaving the system not recording anymore.

This feature can automatically logout the administrator, login a user with no access rights and/or start recording.

1.6.1 Auto Logout Administrator

If the administrator does not press the mouse or press a key within a set period of time, the system will automatically log him/her out.

1. Click the **Configure** button (No. 14, Figure 1-2), point to **System Configure**, and then select **System Idle Protection Setting**. This dialog box appears.

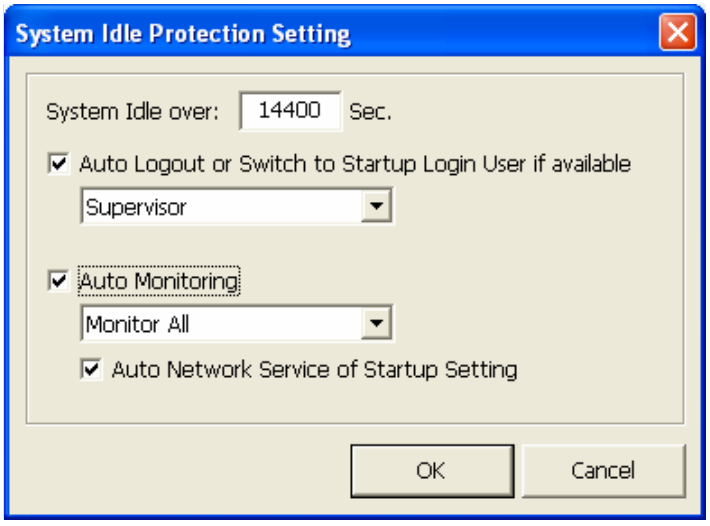


Figure 1-40

2. Enable the **Auto Logout or Switch to Startup Login User if available**, and then select desired option from the drop-down list.
3. In the System Idle Over field, type an idle time between 10 and 14400 seconds, after which Supervisor or Poweruser will be logged out.
4. Click **OK**.

1.6.2 Auto Login User without Access Rights

When the system is started up after an idle time, a specified user with no access right will login. This allows the user to see the system is on and working, but at the same time does nothing with the system. The feature must work with the **Startup Auto Login** function.

1. Click the **Configure** button (No. 14, Figure 1-2), point to **System Configure**, and select **Startup**.
2. In the Startup dialog box, enable **Startup Auto Login**, and click the **Arrow** button beside (Figure 1-17). The Startup Auto Login Setup dialog box appears.
3. Type **ID** and **Password** to set up a user for auto login, and click **OK**.

Figure 1-41

4. In the System Idle Protection dialog box (Figure 1-40), enable **Auto Logout or Switch to Startup Login User if available**, and then select **Supervisor** or **Supervisor, Power User** from the drop-down list.
5. In the System Idle Over field, type an idle time between 10 and 14400 seconds, after which the specified user will be logged in.

1.6.3 Auto Start Recording

If the administrator does not press the mouse or press a key within a set period of time, the system will automatically start recording.

1. In the System Idle Protection dialog box (Figure 1-40), select the **Auto Monitoring** option, and select **Monitoring All**, **Schedule Monitoring**, **I/O Monitoring** or **Camera Monitoring** from the drop-down list. When **Monitoring All** is selected, both **I/O Monitoring** and **Camera Monitoring** will be enabled.
2. In the System Idle Over field, enter an idle time between 10 and 14400 seconds, after which the system will start recording.
3. Enable **Auto Network Service of Startup Setting** for connection to WebCam Server, CenterV2, VSM, Control Center Server, Backup Server (-Failover Server and -Redundant Server) and Backup Center at system startup. To select one or more network connection, see *Customizing Startup Settings* earlier in this chapter.

Note: The feature can monitor keystrokes or mouse clicks, even from IR Remote Control and -Keyboard.

1.7 System Log

System Log provides historical information that can help you track down events, system problems and POS and object counting data. This information is being saved in a database Access format. To view the System Log, click the **ViewLog** button (No. 13, Figure 1-2), and then select **System Log** from the menu. This brings up the Live Log Browser as shown below.

1.7.1 Viewing Event Logs

The Live Log Browser provides five types of event logs. Use the control tabs to switch among them.

[Monitor] Displays information pertaining to motion and I/O events. Double-clicking an alert event in the list will allow you to view related video.

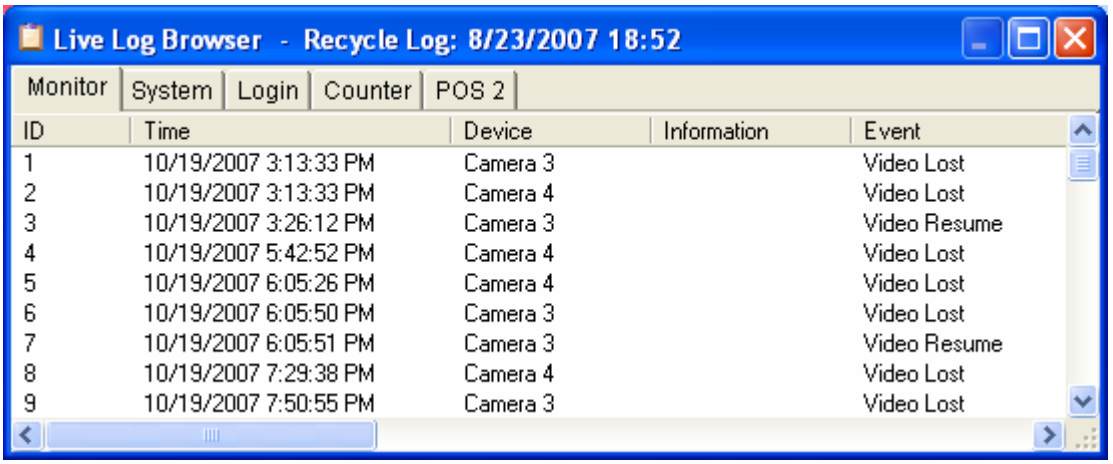

Live Log Browser - Recycle Log: 8/23/2007 18:52
Monitor
System
Login
Counter
POS 2
ID
Time
Device
Information
Event
1 10/19/2007 3:13:33 PM Camera 3 Video Lost
2 10/19/2007 3:13:33 PM Camera 4 Video Lost
3 10/19/2007 3:26:12 PM Camera 3 Video Resume
4 10/19/2007 5:42:52 PM Camera 4 Video Lost
5 10/19/2007 6:05:26 PM Camera 4 Video Lost
6 10/19/2007 6:05:50 PM Camera 3 Video Lost
7 10/19/2007 6:05:51 PM Camera 3 Video Resume
8 10/19/2007 7:29:38 PM Camera 4 Video Lost
9 10/19/2007 7:50:55 PM Camera 3 Video Lost

Figure 1-42

ID: This column shows the event ID number generated by the system.

Time: This column shows the time when a motion or I/O monitor event occurs.

Device: This column shows camera ID or I/O device associated with the event.

Information: This column shows the I/O module number.

Event: These event messages mean:

- **Motion:** Appear if motion occurs in the associated camera.
- **Video Lost:** Appears if video lost occurs in the associated camera.
- **Video Resume:** Appears if video resume in the associated camera.
- **Signal On:** Appears if one of the input device connected to the associated I/O module are activated.
- **Signal Off:** Appears if one of the input device connected to the associated I/O module are terminated.

- ④ **I/O error:** Appears if associated I/O module failed.
- ④ **I/O resume:** Appears if associated I/O module resume to action.
- ④ **Missing Object:** Appears if objects miss from a defined camera view.
- ④ **Unattended Object:** Appears if unattended objects show up within a defined camera view.
- ④ **Intruder:** Appears if there are objects entering a defined region.
- ④ **Disk Full:** Appears if storage space is full.
- ④ **Scene Change:** Appears if the associated camera has been physically tampered.
- ④ **Network Shutdown:** Appears if the network connection is closed.
- ④ **Camera Connection Lost:** Appears if the connection to the associated cameras is lost.
- ④ **Camera Connection Resumed:** Appears if the connection to the associated camera is rebuilt.
- ④ **Tampering Alarm:** Appears if the camera is physically tampered with.
- ④ **Face Count:** Appears if faces are detected under Mask Filter or if no faces are detected under Mask Filter (Inverse Alarm).

[System] This function shows which functions are being enabled or disabled in the -System.

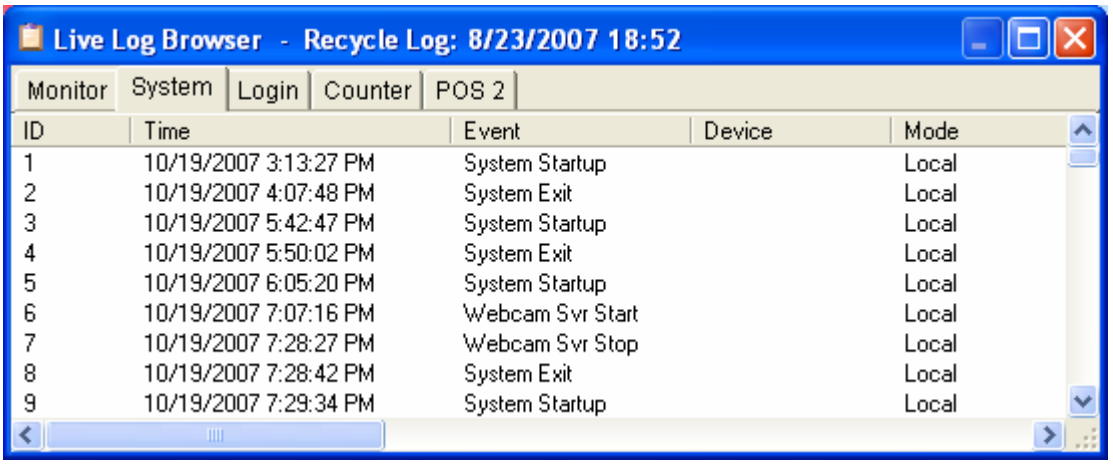

Live Log Browser - Recycle Log: 8/23/2007 18:52
Monitor
System
Login
Counter
POS 2
ID
Time
Event
Device
Mode
1 10/19/2007 3:13:27 PM System Startup Local
2 10/19/2007 4:07:48 PM System Exit Local
3 10/19/2007 5:42:47 PM System Startup Local
4 10/19/2007 5:50:02 PM System Exit Local
5 10/19/2007 6:05:20 PM System Startup Local
6 10/19/2007 7:07:16 PM Webcam Svr Start Local
7 10/19/2007 7:28:27 PM Webcam Svr Stop Local
8 10/19/2007 7:28:42 PM System Exit Local
9 10/19/2007 7:29:34 PM System Startup Local

Figure 1-43

ID: Displays the event ID number

Time: This column shows the time when system event occurs.

Event: This column shows the following messages when associated actions are taken.

- ④ **Schedule Start / Stop:** Appears when a user starts or stops the monitoring schedule.
- ④ **Auto Reboot:** Appears when the system performs auto rebooting function.
- ④ **System Start / Exit:** Appears when a user starts or stops -System.
- ④ **Start / Stop Monitor All:** Appears when a user starts or stops all cameras' monitoring functions.
- ④ **Start / Stop Monitor:** Appears when a user starts or stops the individual camera's monitoring function. The camera number will appear in Device column.

- ④ **IO Monitor Start / Stop:** Appears when a user starts or stops the individual I/O module's monitoring function. The I/O module number will appear in the Device column.
- ④ **WebCam Svr Start / Stop:** Appears when a user starts or stops WebCam Server.
- ④ **Connect to Center Start / Stop:** Appears when the -System connects or disconnects with the Security Center.
- ④ **Connect to Center V2 Start / Stop:** Appears when the -System logs in or out Center V2.
- ④ **Connect to VSM Start / Stop/Net Down / Net Resume:** Appears when the -System logs in or out VSM; when the connection of both fails or resumes.
- ④ **Connect to SMS Start / Stop / Net Down / Net Resume:** Appears when the -System logs in or out the SMS server; when the connection of both fails or resumes.
- ④ **Send Email Alert:** Appears when an e-mail alert is sent out.
- ④ **Send SMS Alert:** Appears when an SMS alert is sent out.
- ④ **Send Hotline Alert:** Appears when a Hotline alert is sent out.
- ④ **Windows Shutdown:** Appears when Windows is closed.
- ④ **Recycle:** Appears when the -System recycles event files to increase storage space.
- ④ **Auto-Reboot:** Appears when Windows is automatically rebooted.

Device: This column shows the individual camera number.

Mode: This column shows whether actions are being taken in local side or remote side.

[Login] This function shows whom and when has logged in and out the -System and WebCam server.

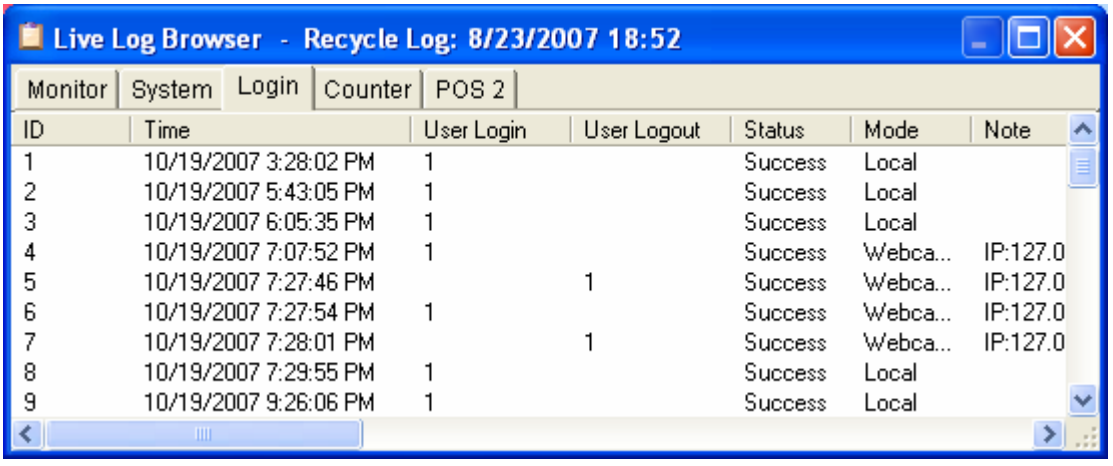

Live Log Browser - Recycle Log: 8/23/2007 18:52
Monitor
System
Login
Counter
POS 2
ID
Time
User Login
User Logout
Status
Mode
Note
1 10/19/2007 3:28:02 PM 1 Success Local
2 10/19/2007 5:43:05 PM 1 Success Local
3 10/19/2007 6:05:35 PM 1 Success Local
4 10/19/2007 7:07:52 PM 1 Success Webca... IP:127.0
5 10/19/2007 7:27:46 PM 1 Success Webca... IP:127.0
6 10/19/2007 7:27:54 PM 1 Success Webca... IP:127.0
7 10/19/2007 7:28:01 PM 1 Success Webca... IP:127.0
8 10/19/2007 7:29:55 PM 1 Success Local
9 10/19/2007 9:26:06 PM 1 Success Local

Figure 1-44

ID: Shows the event ID number.

Time: This column shows the time when Login event occurs.

User Login: This column shows the ID of the login user.

User Logout: This column shows the ID of the logout user.

Status: This column shows whether login or logout attempts were successful or failed.

Mode: This column shows the following messages:

- ④ **Local:** Appears if a user logs in or logs out the Main System.
- ④ **WebCam:** Appears if a remote client logs in or logs out the WebCam server.
- ④ **Remote DVR:** Appears if a Control Center operator logs in or logs out via the Remote DVR service.
- ④ **Remote Matrix:** Appears if a Control Center operator remotely logs in or logs out via the Matrix View service.
- ④ **Remote Desktop:** Appears if a Control Center operator logs in or logs out via the Remote Desktop service.

Note: This column shows the IP address of the client server.

[Counter] This function shows the information and result of -System's counter function.

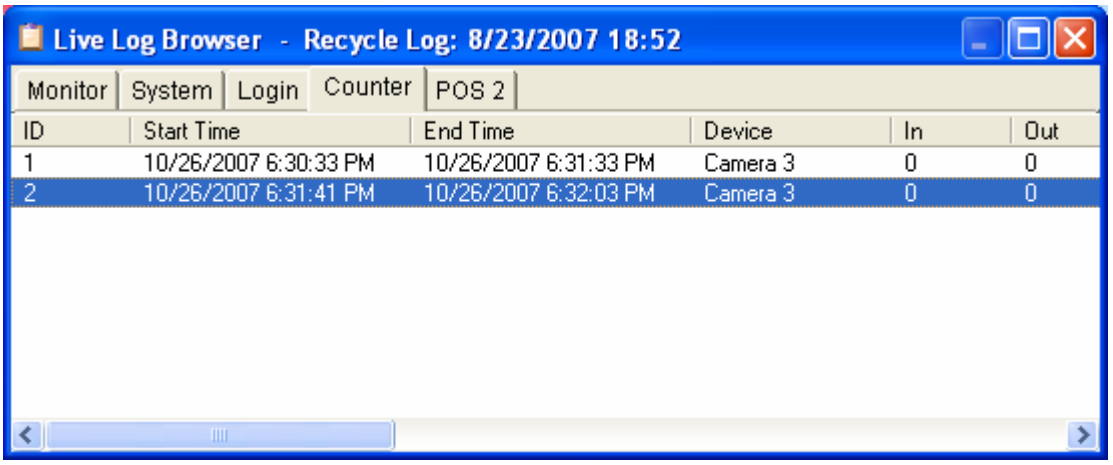


Figure 1-45

ID: This column shows the event ID number.

Start Time: This column shows the time when -System's counter function is activated.

End Time: This column shows the time when -System's counter function is terminated.

Device: This column shows the camera that performs counter function.

In: This column shows the "In" result of -System's counter function.

Out: This column shows the "Out" result of -System's counter function.

[POS] This function shows the POS event information. Double-clicking on the log list will allow you to view related video in ViewLog or Quick Search (depending on the video player you selected in the System Log Setting dialog box. See Figure 1-47).

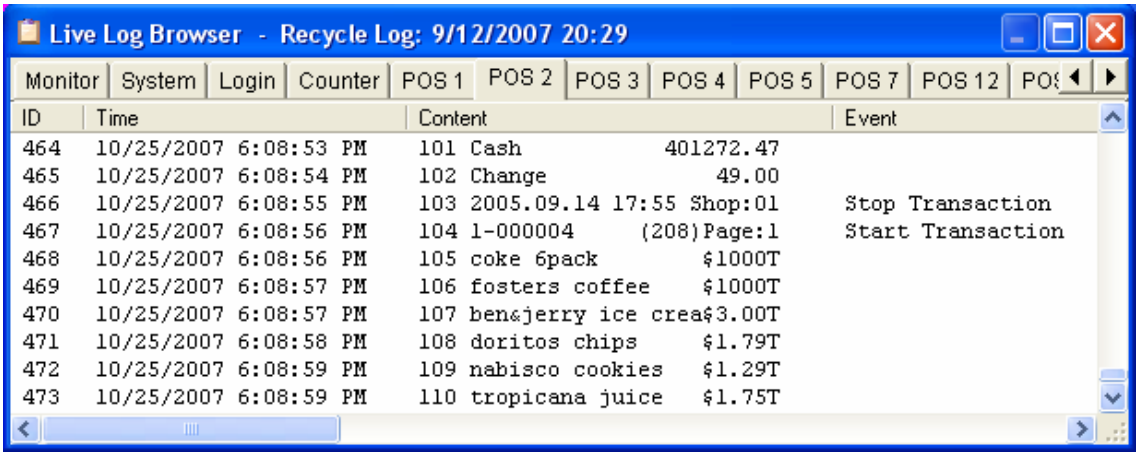


Figure 1-46

ID: This column shows the event ID number.

Time: This column shows the time when POS event occurs.

Content: This column shows the action taken in the POS device.

Event: This column shows the following messages.

- ④ **Start Transaction:** Appears when sales transaction starts.
- ④ **Stop Transaction:** Appears when sales transaction ends.
- ④ **Void Transaction:** Appears if an item is being void from the sales transaction.
- ④ **Cash Drawer Open:** Appears if the cash drawer is opened.
- ④ **Filter 1-15:** Appears if the sales transaction matches the defined condition 1 to 15.

Note: This column is currently not being used.

1.7.2 Setting Event Logs

You can define several event log settings, specifying which event log to be recorded, the interval time to write the log into the system, video player, and the number of days to keep the logs. To access these log settings, click the **Configure** button (No.14, Figure 1-2), select **System Configure** and select **System Log Setting** to display the following dialog box.

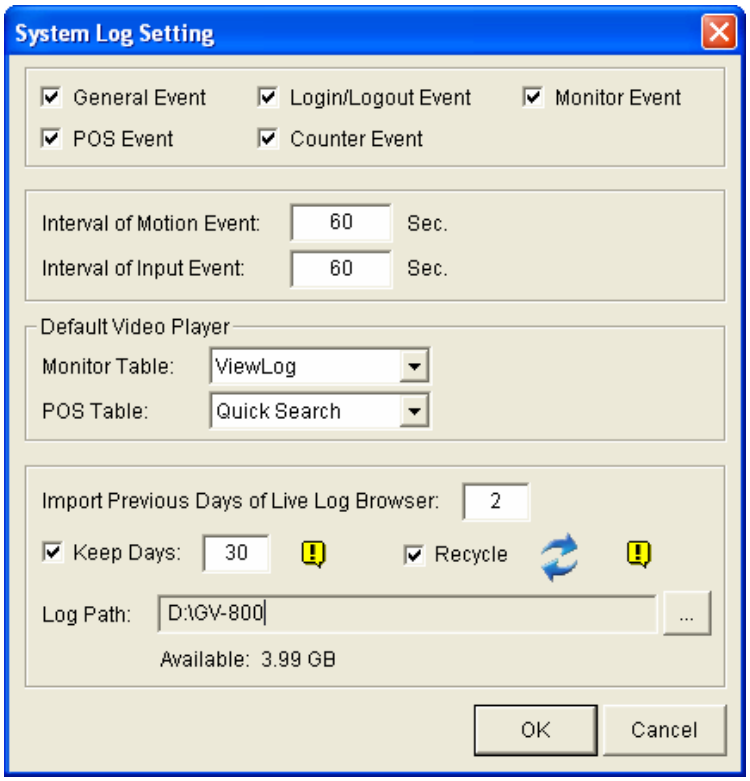


Figure 1-47

④ **General Event:** Records system startup/exit, network server start/stop, and recording start/stop.

④ **Login/Logout Event:** Records the login/logout activities of the local user to -System and WebCam Server.

④ **Monitor Event:** Records motion-triggered and I/O-triggered events. For this feature to work, you must enable the **Register Motion Event** option in Figure 1-11 or the **Register Input Event** option in Figure 6-7 in Chapter 6.

④ **POS Event:** Records POS transaction data.

④ **Counter Event:** Records counting results.

④ **Interval of Motion Event:** Specifies the log interval between motion-triggered events. This setting could prevent the System Log growing too big when trying to log all events under a motion-intensive surveillance area.

④ **Interval of Input Event:** Specifies the log interval between I/O-triggered events.

[Default Video Player]

④ **Monitor Table:** Specifies the playback software for monitor events. For details on each playback application, see Chapter 5.

④ **POS Table:** Specifies the playback software for POS events.

[Import Previous Days of Live Log Browser] Specifies how many days of data to be loaded into the System Log.

④ **Keep Days:** Set the number of days to keep logs.

④ **Recycle:** Enable the system to delete old log files to make space for new files when the space of assigned Log Path is below 500 MB.

④ **Log Path:** Click the **…** button to specify a storage path. The default log path is: :\ folder\database. The available free space of the storage path will be displayed below.

1.7.3 Searching Event Logs

To search for log data, click the icon on the upper left corner of the Live Log Browser to bring up the Advanced Log Browser. See *Advanced Log Browser* in Chapter 4.

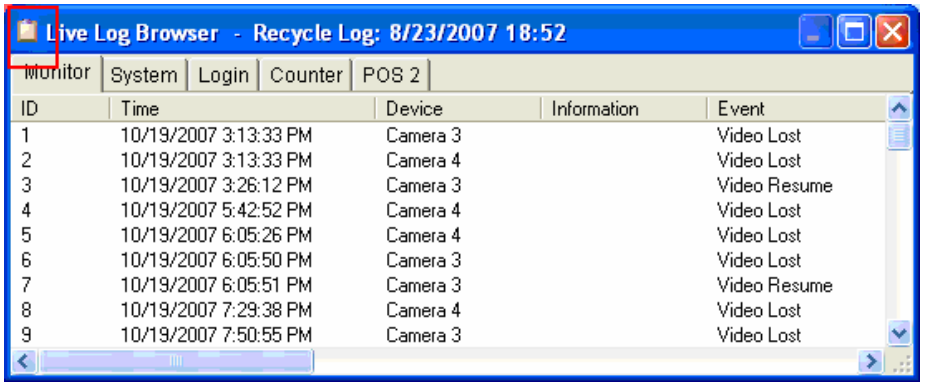

Live Log Browser - Recycle Log: 8/23/2007 18:52
Monitor
System
Login
Counter
POS 2
ID
Time
Device
Information
Event
1 10/19/2007 3:13:33 PM Camera 3 Video Lost
2 10/19/2007 3:13:33 PM Camera 4 Video Lost
3 10/19/2007 3:26:12 PM Camera 3 Video Resume
4 10/19/2007 5:42:52 PM Camera 4 Video Lost
5 10/19/2007 6:05:26 PM Camera 4 Video Lost
6 10/19/2007 6:05:50 PM Camera 3 Video Lost
7 10/19/2007 6:05:51 PM Camera 3 Video Resume
8 10/19/2007 7:29:38 PM Camera 4 Video Lost
9 10/19/2007 7:50:55 PM Camera 3 Video Lost

Figure 1-48

1.8 Recording Schedule

You can program recording, I/O devices, and Center V2 services to turn on and off at specific time each day. Click the **Schedule** button (No.15, Figure 1-2) and select **Schedule Edit** to display the following window.

The window has three major tabs:

④ **Video Schedule:** A schedule starts the surveillance system automatically.

④ **I/O Schedule:** A schedule starts I/O surveillance automatically.

④ **Center V2 Schedule:** A schedule starts the connection to Center V2 services automatically.

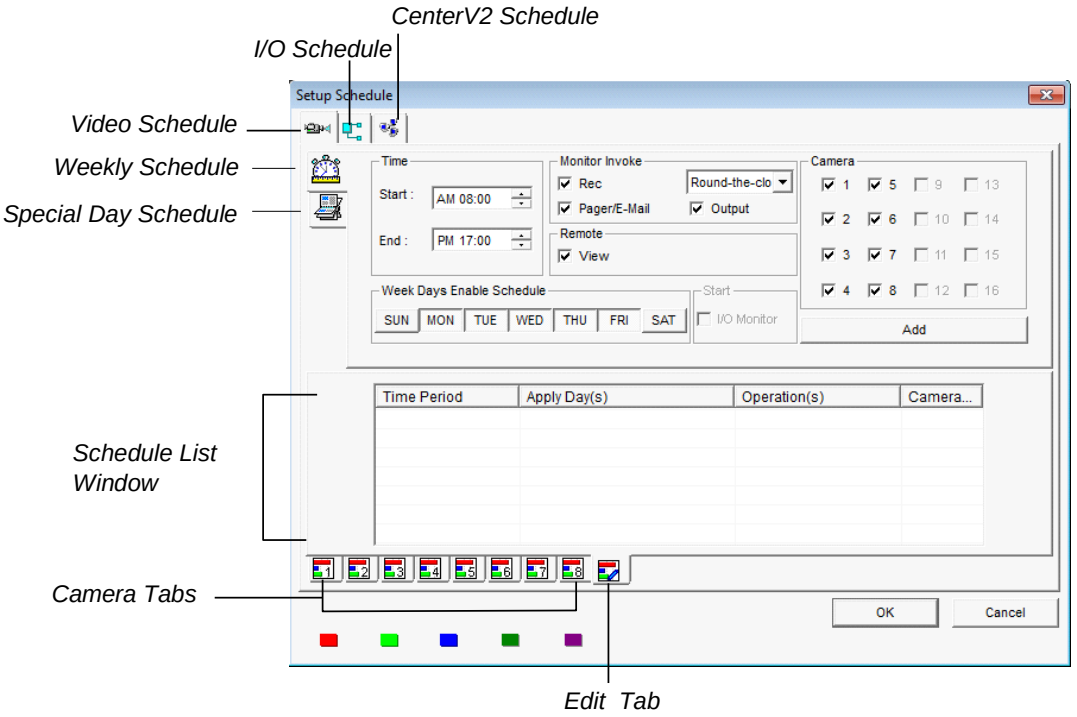


Figure 1-49

Note: You can add the schedule settings using the Camera Tabs or the Edit Tab. To modify the settings, you have to use the Edit Tab.

1.8.1 Video Schedule

Setting up a Video Schedule

1. Set your surveillance preferences:

   [Time] Enter the starting and ending time of the schedule.

   [Monitor Invoke] Sets alert methods on motion detection.

   ④ **Rec:** Records while monitoring. Select the recording mode to be Motion Detection or Round-the-Clock.

   ④ **Pager/E-Mail:** Sends pager or e-mail alerts on motion detection.

   ④ **Output:** Triggers the corresponding I/O devices on motion detection. To set up I/O devices, see *Adjusting Individual Camera* earlier in this chapter.

   [Remote] Allows remotely accessing live video from the WebCam server on the scheduled time.

   [Week Days Enable Schedule] Select days for the schedule.

   [Camera] Applies the settings to selected cameras.

2. Click the **Add** button to apply above settings. The schedule that you just edit will be displayed on the Schedule List Window.
3. Repeat above steps to set up more schedules.
4. Click **OK**.

You will see different color bars being displayed on the Schedule List Windows when you click the Camera Tabs. Each color stands for a setting.

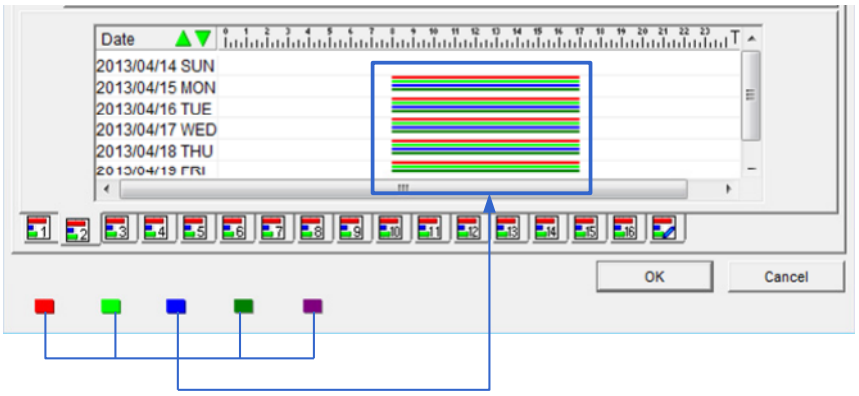


Figure 1-50

④ **Red:** Recording enabled.

④ **Green:** Pager/E-mail notification enabled.

④ **Blue:** Live view from the WebCam server accessible.

④ **Jade:** I/O monitor enabled.

④ **Purple:** Center V2 schedule enabled.

Modifying a Video Schedule

1. Click the **Edit** tab .
2. Click the desired schedule to highlight it in the Schedule List window.
1. Change the settings of surveillance preferences. You can refer to the previous section of *Setting up a Video Schedule* in this chapter.
2. Click the **Modify** button to apply the changes to your schedule.
3. Click **OK**.

Deleting a Video Schedule

1. Click the **Edit** tab .
2. Click the desired schedule to highlight it in the Schedule List window.
3. Press the **Delete** key on your keyboard.
4. Click **OK**.

1.8.2 Special Days Schedule

1. Click the **Special Day Schedule** tab.
2. All settings are the same as those in Video Schedule, except the following section. Use the drop-down list and select a date from the pop-up calendar. Click **Apply** to add the date to the schedule.

Figure 1-51

1.8.3 I/O Schedule

Set up a schedule to activate the monitoring of I/O devices automatically. All settings are the same as those in Video Schedule, except the following section. After setting up time and dates, select the **I/O Monitor** option to activate the schedule.

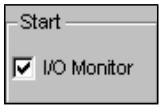


Figure 1-52

1.8.4 Center V2 Schedule

Set up a schedule to connect to Center V2 services automatically. All settings are the same as those in Video Schedule, except the following section. After setting up scheduled time and dates, select the **Center V2** option to activate the schedule. For details on Center V2, see Chapter 1 in *-CMS Series User's Manual*.

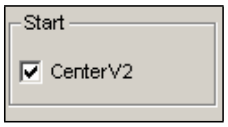


Figure 1-53

Note: If you select the **Center V2** option without setting up the Center V2 schedule and later enable the Center V2 server, the connection to Center V2 will be stopped automatically after 15 minutes. For this problem, please complete the setup of Center V2 schedule or clear the **Center V2** option.

1.9 Schedule Center

The Schedule Center allows you to set up a schedule to automatically compact video events, merge video events, and back up the system settings.

1.9.1 Compacting Video Events

The Video Compacting feature helps you to save storage space by extracting key frames from the recorded files. After the extraction, the recorded files will be composed of key frames only. This can significantly reduce the file size. The Video Compacting action is enabled on a specific weekly schedule.

Note:

1. The audio files cannot be compacted.
2. If a file is in playback when it is supposed to be compacted, the compacting will not occur. The compacting will be started the next time when the -System is scheduled to compact video files.
3. Compacting the recorded files to key frames only will affect the smoothness of the playback, but will not result in data loss since key frame contains the complete image and only the intermediate frames between key frames are deleted.

Setting up a Compacting Schedule

1. Click the **Schedule** button, select **Schedule Center** and select **Compacting Video Events**.

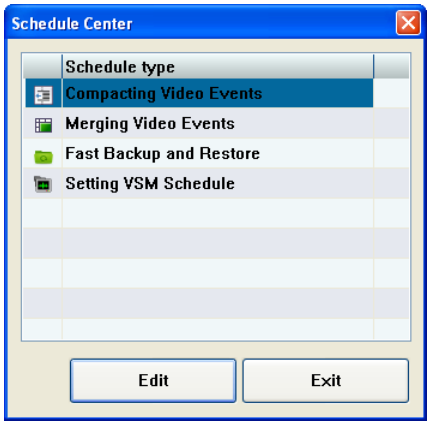


Figure 1-54

2. Click **Add schedule**. This dialog box appears.

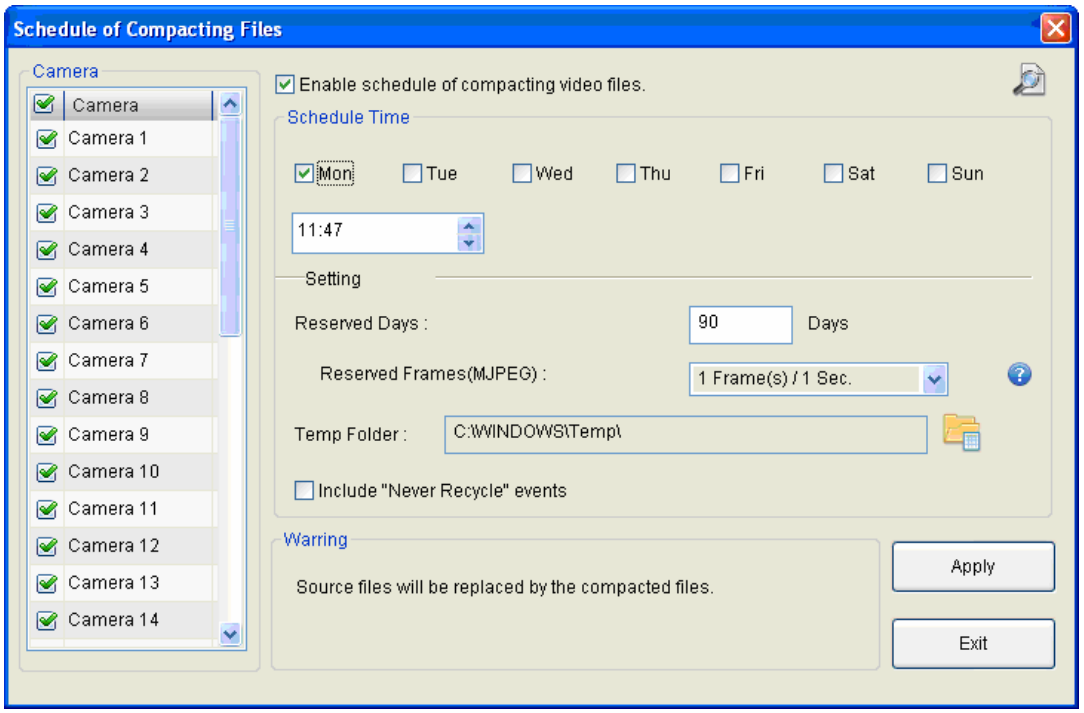


Figure 1-55

3. Select the desired camera individually, or select **Camera** to check all the cameras from the camera list.
4. Select **Enable schedule of compacting video files**.
5. In the Schedule Time section, specify the day and time to compact the video files.
6. In the Setting section, specify the options below.

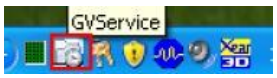
   ④ **Reserved Days:** The number of days that the original video files are reserved. For example, if you choose to reserve the video files for 2 days, the system will keep the original video files for the last two days (recorded today and yesterday), and compact all the files earlier. The minimum value is to reserve 1 day.

   ④ **Reserved Frames (MJPEG):** Since every frame is a key frame for MJPEG codec, you should specify the number of frames per second you desire to reserve for the video files compressed with MJPEG. The default value is 1 frame per second.

   ④ **Temp Folder:** The temporary storage path for the video files to be compacted.

   ④ **Include "Never Recycle" events:** This option enables the video files that are set to be "never recycle" to be compacted.

7. Click **Exit**.

After setup is completed, the Service icon appears on the Windows notification area as shown below. 

The Service program allows the video compacting to run automatically without the starting the -System.

When the -System starts to compact video files at the time you specified, the following Compacting List will pop up, displaying the information such as the camera number, the processing status, the processing time and the number of files that are being compacted.

To view the log files of video compacting, click the icon in the bottom of the window.

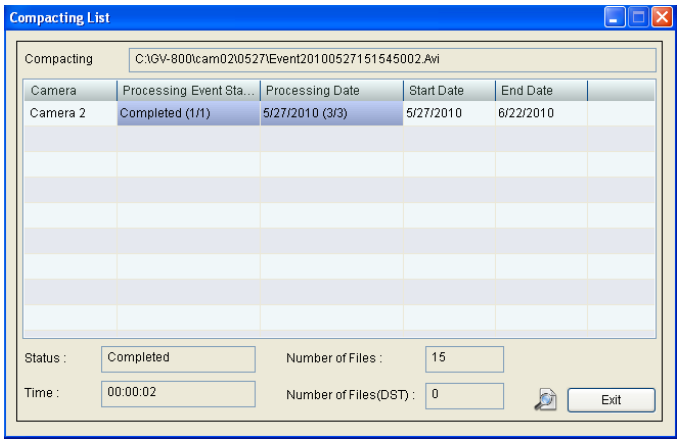


Figure 1-56

Viewing Compacted Video Files

After the video compacting, the compacted files will replace the original files and become the video events you view on ViewLog. After selecting a camera and date you specified for video compacting, you would see three types of icons on the Video Event list.

Icons appearing under the scheduled-compacting date	Description
Key	The compacted file.
Never-Recycle	The compacted file of the Never-Recycle event remains the same icon.
Tick	The video file has failed to be compacted because the file was being played back when it was supposed to be compacted.

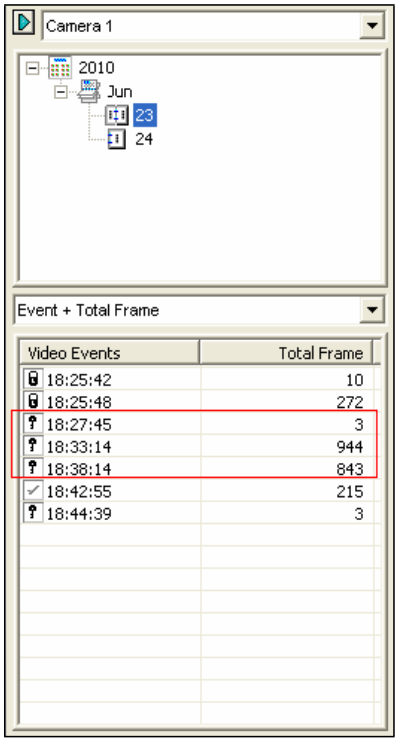


Figure 1-57

1.9.2 Merging Video Events

You can program the file merging and exporting to begin on a specific date or on a daily schedule. The schedule is helpful when computer sources are busy at monitoring or detection, it allows you to assign the file merging and exporting after working hours.

Setting up a Merging Schedule

1. Click the **Schedule** button, select **Schedule Center** and select **Merging Video Events**.

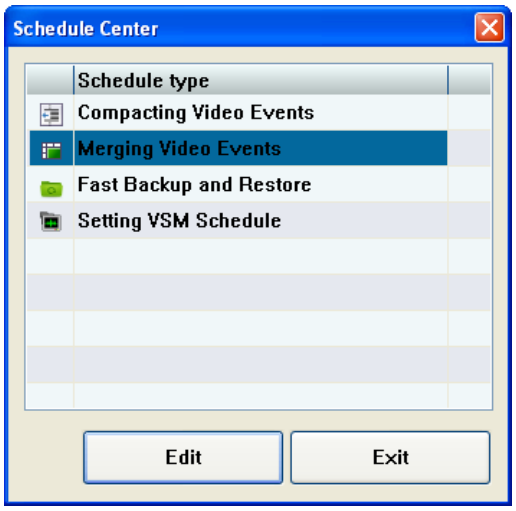


Figure 1-58

2. Click **Edit**. This dialog box appears.

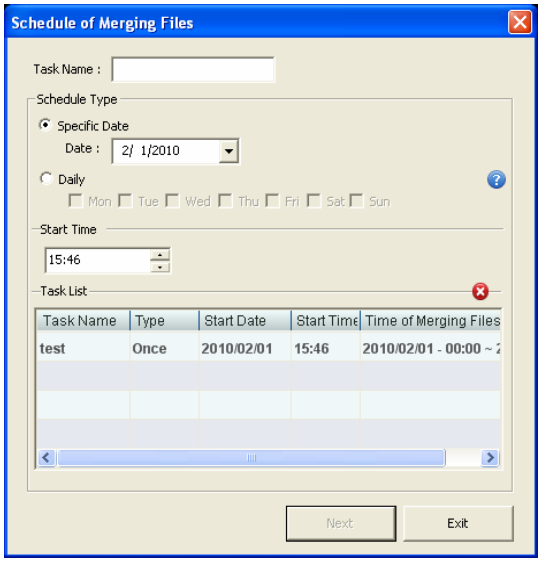


Figure 1-59

3. In the **Task Name** field, name the schedule.
4. In the **Schedule Type** section, select one of the types:
   - ④ **Specific Date:** The file merging only begins on the specified date. You can further choose to merge files from a specific time period on the specified date in step 7.
   - ④ **Daily:** The file merging begins on the selected days every week. The Daily schedule merges the files of the day previous to the selected day. For example, if you select Tue, Thu and Sat to begin file merging. The files of Mon, Wed and Fri will be merged on those selected days respectively.
5. In the **Start Time** section, specify the time of day to begin the file merging.
6. Click **Next**. This dialog box appears.

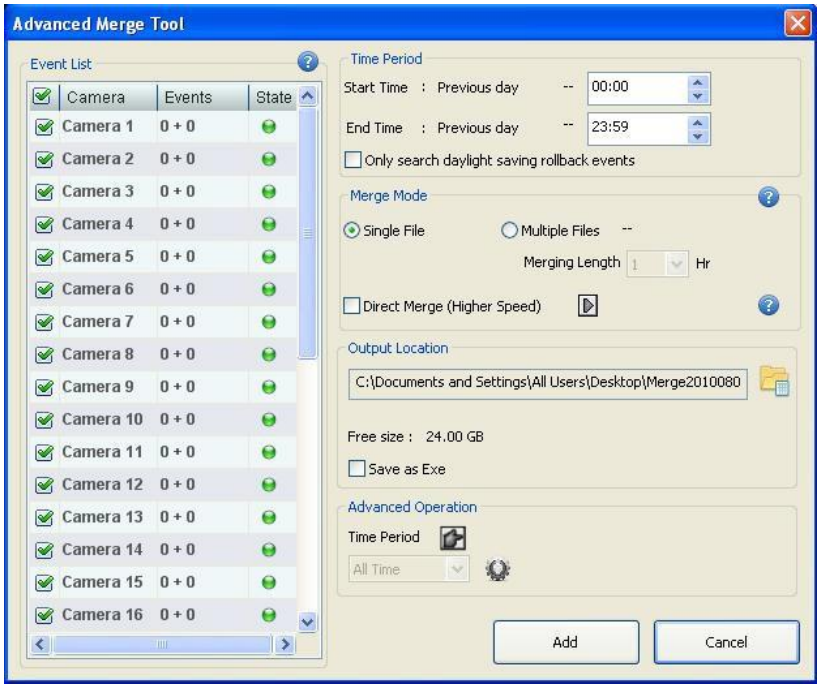


Figure 1-60

7. In the **Time Period** section, specify Start and End time to locate files. The number of video and audio files for each camera found within the specified time is displayed in the camera list on the left. For example, “Camera 9 18+0” means the Camera 9 has created 18 video files and 0 audio files within the specified time. By default you can only merge the files of one day.
8. In the **Merge Mode** section, select one of the merging methods:
   - ④ **Single File:** Merges several AVI files into a single file. The maximum size of the merged file is 2 GB for FAT32 file system and 4 GB for NTFS file system. If the merged file exceeds the limit of Windows file system, it will be split up into another file.

- ④ **Multiple Files:** Merges AVI files into several files of a specific duration. After specifying the duration, you can see the number of merged files will be created.
- ④ **Direct Merge (Higher Speed):** The merging method only joins video files together without the inclusion of their video effects, such as privacy masks, watermarks, time stamps, GPS data and etc.
  - ⌘ Using the Direct Merge to merge several AVI files into a single file, also select **Single File**.
  - ⌘ Using the Direct Merge to merge AVI files based on the specified duration, also select **Multiple Files**.
  - ⌘ To merge audio and video together, click the arrow button and select **Include Audio**.

  The Direct Merge is faster than the other two merging methods, because the video effects are excluded.

9. In the **Output Location** section, specify the storage location of merged files, and select whether to save merged files in EXE format.
10. Click **Add** to create the schedule task.

1.9.3 Setting Backup Schedule

You can set up a schedule to regularly back up the configurations in the Main System. The backup settings can be restored to the current system or imported to another -System.

1. Click the **Schedule** button, and select **Schedule Center**. This dialog box appears.

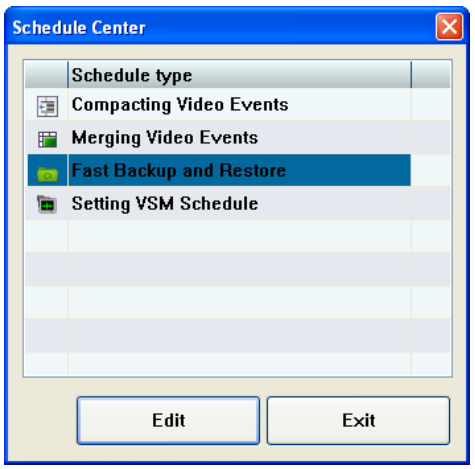


Figure 1-61

2. Select **Fast Backup and Restore** and click **Edit**. This dialog box appears.

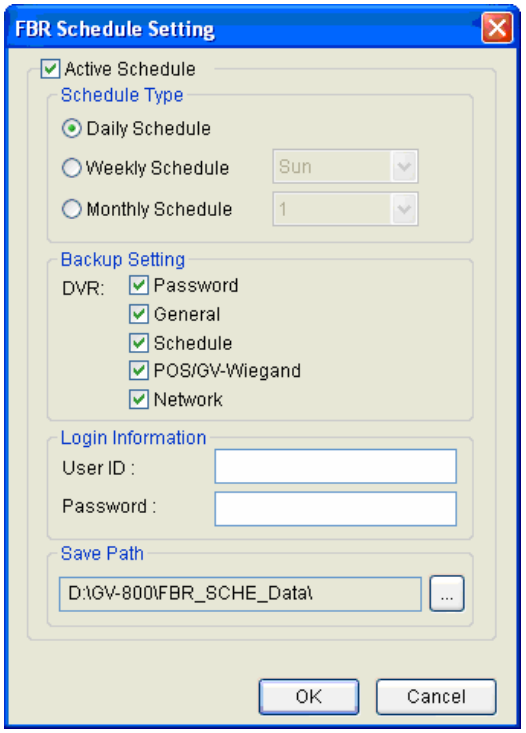


Figure 1-62

3. Select **Active**.
4. Under the **Schedule Type** section, choose a backup schedule.
   - ④ **Daily Schedule:** Backs up the system configurations daily.
   - ④ **Weekly Schedule:** Select a day of the week from the drop-down list to back up the system configurations.
   - ④ **Monthly Schedule:** Select a day of the month from the drop-down list to back up the system configurations. Note that if you have selected 31, and the particular month does not have the 31st day, the system will skip backup for that month.
5. Under the **Backup Setting** section, select the settings you want to back up.
6. Type the ID and Password of your login account.
7. Under the **Save Path** section, specify a file path to store the settings.
8. Click **OK** to save the settings.

After setup is completed, the Service icon appears on the Windows notification area as shown below.

The Service program allows the backup to run automatically without starting the -System.

For details on how to restore the system, see *Backing Up and Restoring Settings* in Chapter 11.

Note: Backup will be performed at the time when you first set up the function. For example, if the time when you click OK to apply a daily backup schedule is 11:30am, the system will perform backup at 11:30am everyday.

1.9.4 Setting VSM Schedule

You can set up a schedule to activate the connection to Vital Sign Monitor (VSM) on a specific date or on a weekly schedule.

Note: For details on setting up the connection to the VSM, see Chapter 3 in *-CMS Series User's Manual*.

---

1. Click the **Schedule** button, and select **Schedule Center**. This dialog box appears.

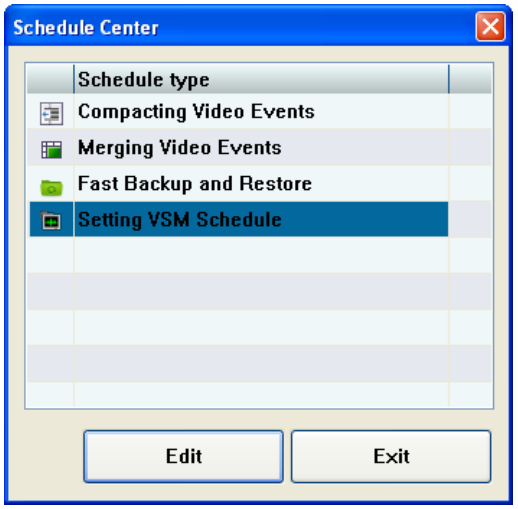


Figure 1-63

2. Select **Setting VSM Schedule** and click **Edit**. This dialog box appears.

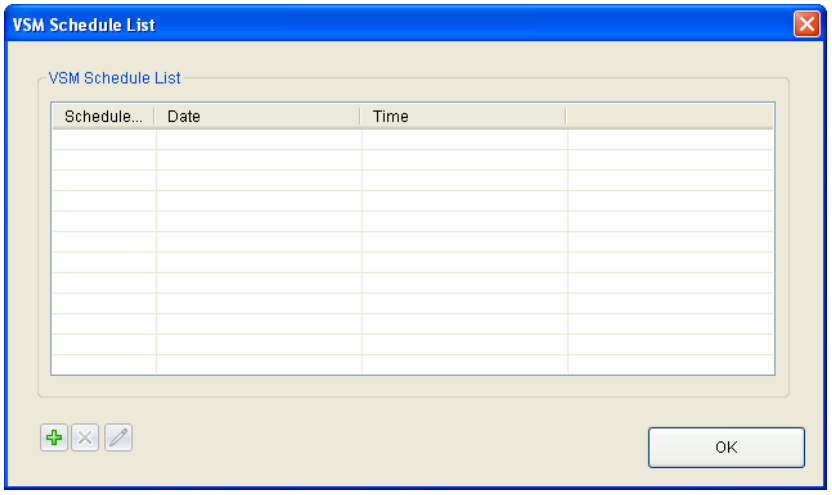


Figure 1-64

3. To add a new schedule, click the **Add** button . This dialog box appears.

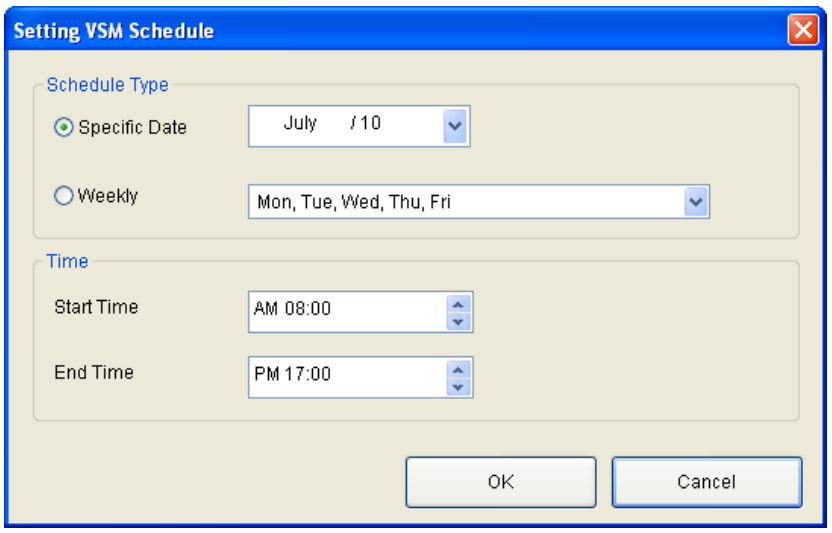


Figure 1-65

4. Select to activate VSM on a **Specific Date** or select **Weekly** to set up a weekly schedule.
5. Set a **Start Time** and an **End Time** for the Specific Date or Weekly schedule.
6. Click **OK** to add the schedule.

You can add multiple schedules by clicking the **Add** button and repeating the steps above.

1.10 Alert Notification

When events occur, you can receive alert notification through e-mails, SMS messages, pagers or telephones. Follow the steps below to enable alert notification and select the event types to receive notification.

The events that can trigger alert notification include: Video Lost, Recording Error, Disk Full, Motion Detection, I/O Trigger, Scene Change, Intruder Event, Missing Object, Unattended Object. POS Loss Prevention, Scene Change, Crowd Detection, Advanced Unattended Object, Advanced Scene Change Detection, Advanced Missing Object and Face Detection.

1. Click the **Configure** button (No.14, Figure 1-2), select **System Configure** and click **Send Alerts Approach Setup**. This dialog box appears.

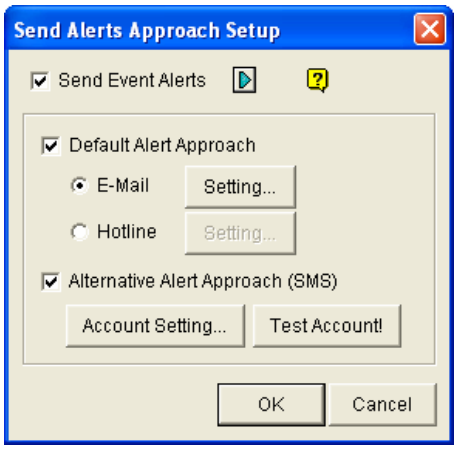


Figure 1-66

2. To enable alert notification, select **Send Event Alerts**.

3. To specify the types of events to receive alert notification, click the arrow button next to **Send Event Alerts** and select the alert types. Some alerts are only available when the alert settings are activated.

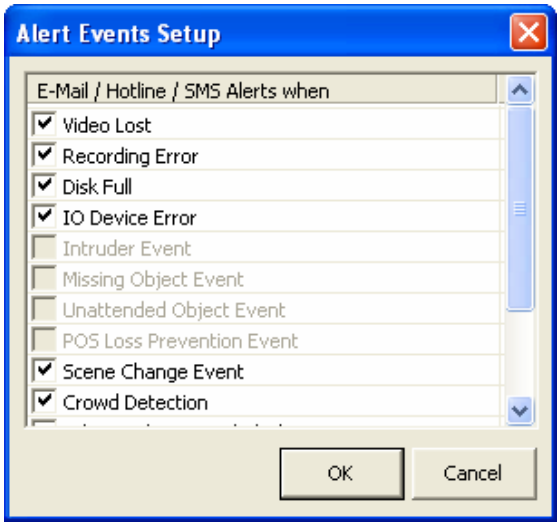


Figure 1-67

4. Click **OK**.
5. To send e-mail, hotline or SMS alerts when motion is detected, click **Invoke to Send Alerts** in the **Camera Configure** (F9) dialog box. You can select specific cameras for this application or click the Finger button to apply the setting to all the cameras. See Figure 1-11. For related settings, see*, Invoke to Send Alerts* and options earlier this chapter.
6. To receive notification by e-mail or hotline, select **Default Alert Approach** and select **E-Mail** or **Hotline**. To receive notification by SMS, select **Alternative Alert Approach (SMS)**. To see how to set up e-mail server or hotline service, refer to the sections below. To see how to set up SMS notification, refer to Chapter 10 for more details.

1.10.1 Setting Email Server

To send e-mail notification, you need to first set up your mail server as described below:

1. In the Send Alerts Approach Setup dialog box (Figure 1-66), enable **Default Alert Approach**, select **E-Mail** and click the **Setting** button. This dialog box appears.

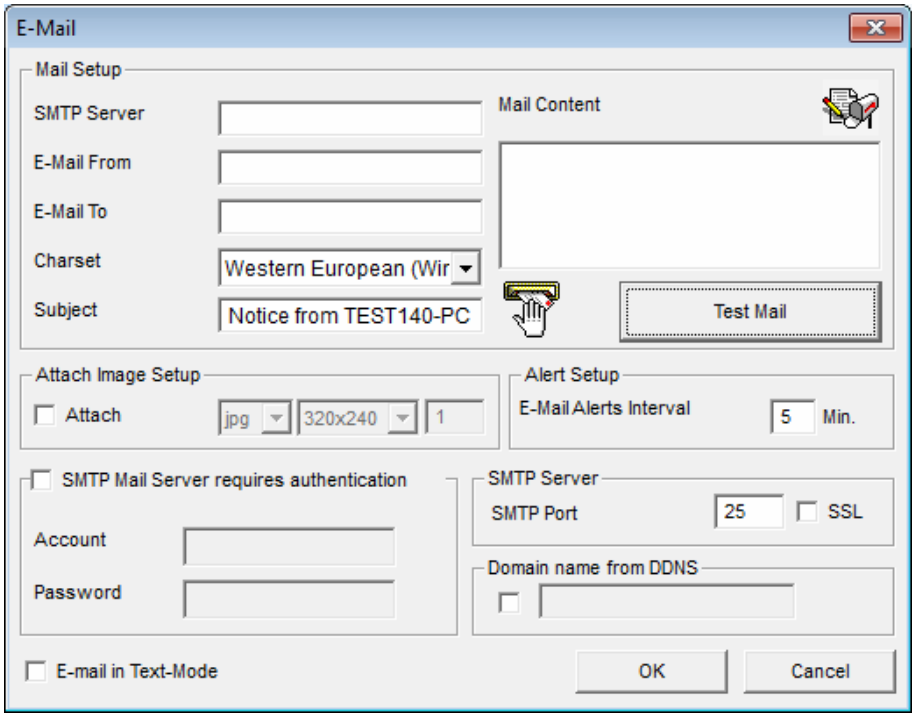


Figure 1-68

2. In the Mail Setup section, set up the following fields:
   - ④ **SMTP Sever:** Type your mail server's URL address or IP address.
   - ④ **E-Mail From:** Type the sender's e-mail address.
   - ④ **E-Mail To:** Type recipients' e-mail addresses. For multiple recipients, add a semicolon between each e-mail address.
   - ④ **Charset:** Select the character set for outgoing e-mails.
   - ④ **Subject:** Type a subject that comes with the alert message.
3. Click the **Test Mail Account** button to send a test e-mail and see whether the setup is correct. If the connection attempt fails, you may also need to check the settings of **SMTP Mail Server requires authentication** and **SMTP Server** described below.

Other options on the E-Mail dialog box:

[Attach Image Setup] Select **Attach** to include up to 6 snapshots in the e-mail. The image format and size are selectable from drop-down lists.

[Email-Alerts Setup] Specify the time interval between e-mail alerts. This option can prevent e-mails from being sent frequently. The default interval is 5 minutes (configurable from 0 to 60 minutes). For example, if motion lasts for more than 15 minutes, it means that you will receive 3 e-mails at least. If motion lasts for less than 5 minutes, you will receive one e-mail only.

[SMTP Mail Server requires authentication] If the SMTP mail server needs authentication for login, select this option and type your account name and password.

[SMTP Server] Keep the default port 25 which is common for most SMTP servers. However webmail providers such as Yahoo and Hotmail generally use different SMTP port. In this case, check your e-mail provider for the SMTP port number. Select **SSL** if your e-mail server requires the SSL authentication for connection.

[Domain Name from DDNS] This option generates URL links for remote video playback in the sent e-mails. For this function to work, enter the fixed IP address or domain name of the -System, and enable **WebCam Server**.

[E-mail in Text Mode] When **WebCam Server** is enabled, your e-mail alert will be sent in HTML format. If you want to send the e-mail alert in pure text format, select this option.

1.10.2 Setting Hotline Services

When events occur, you can receive notification by a text or voice message through pagers or telephones.

1. In the Send Alerts Approach Setup dialog box (Figure 1-66), enable **Default Alert Approach**, select **Hotline** and click the **Setting** button. This dialog box appears.

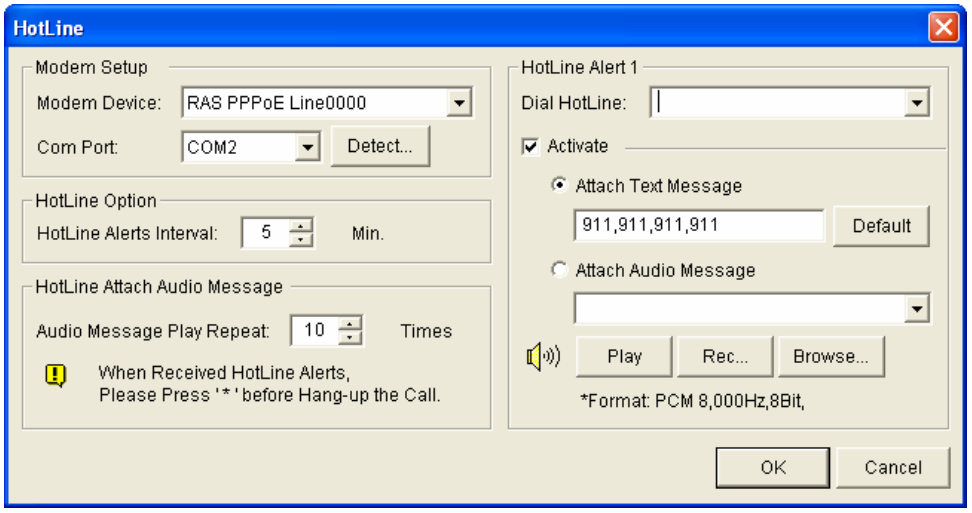


Figure 1-69

[Modem Setup] Select the dialup modem installed on the computer of the -System, and the COM port that is connected. Click the **Detect** button to test the connection with the modem.

Note: Internal modems (PCI or ISA) are not recommended.

[Hotline Alert x] The event can be set to trigger up to 3 units of telephones and pagers. A text message may be sent to the pager.

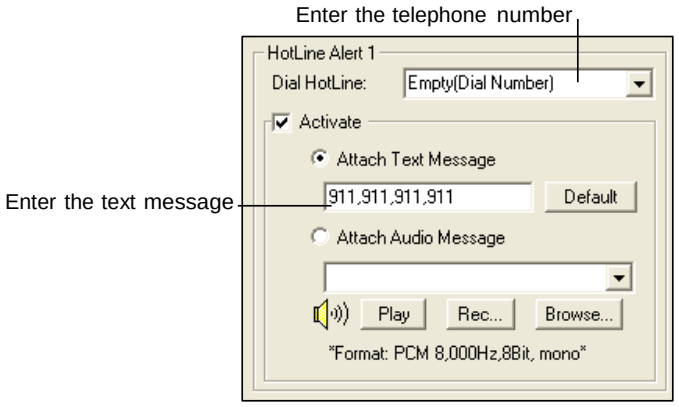


Figure 1-70

1. In the **Dial HotLine** drop-down list, type the telephone or pager number.
2. Select **Activate**.
3. Select **Attach Text Message** and type the text messages to be sent to a pager.
4. The system allows you to send a custom sound file to the telephone. For this operation a microphone must be installed on the computer of the -System. To record a sound file, follow these steps:

   a. Click the **Rec** button. This dialog box appears.

Figure 1-71

   b. Click the **Record** button to start recording. Speak the message script clearly to the microphone. Click **Stop** button when it is done.

   c. Click the **Play** button to listen to the recording. To save this sound file, click **File**, select **Save as**, and then click the **Change** button. This Sound Selection dialog box appears.

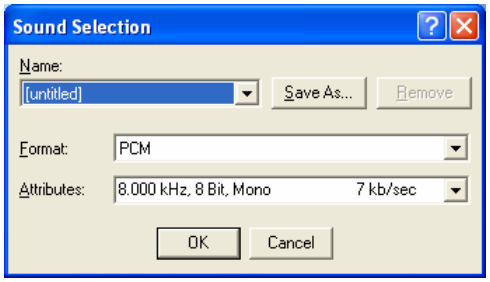


Figure 1-72

   d. Select ***PCM 8,000 Hz, 8-bit Mono*****,** the only format supported for this feature, and then click **OK**.

5. To find a sound file, click the **Browse** button to locate the file. Add the path of the file to the field, and the file will be sent with the telephone calls.

[Hotline Option] Specify the interval between hotline alerts. The option is useful for the frequent event occurrence by which any event triggers during the interval period will be ignored.

[Hotline Attach Audio Message] Specify how many times to repeat the audio message when a telephone call is made to you.

1.11 PTZ Control

With the PTZ control panel, you can control PTZ functions, e.g. pan, tilt, zoom, focus and preset points. This control panel will not appear, unless at least one PTZ camera is connected to the system.

Adding a PTZ Camera

For the IP Camera, skip steps 1 to 3 and start from the step 4.

1. Click **Configure** button (No. 14, Figure 1-2), select **Accessories**, select **PTZ Device** and select **Add / Remove PTZ**. This dialog box appears.

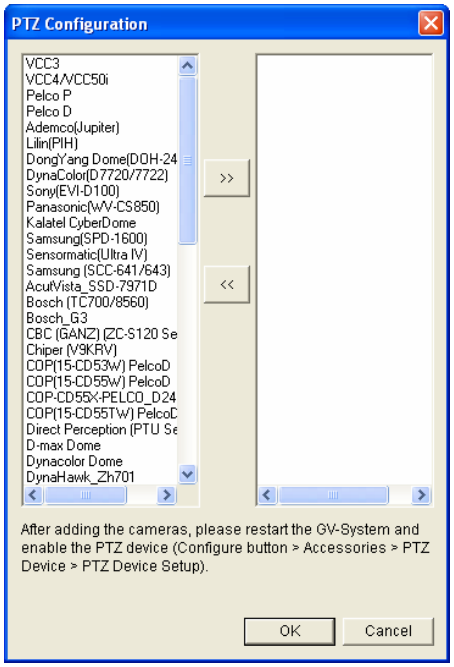


Figure 1-73

2. Select the brand of your camera, and click the >> button.
3. Click **OK** and restart the -System.
4. Click **Configure** button (No. 14, Figure 1-2), select **Accessories**, select **PTZ Device** and select **PTZ Device Setup**. This dialog box appears.

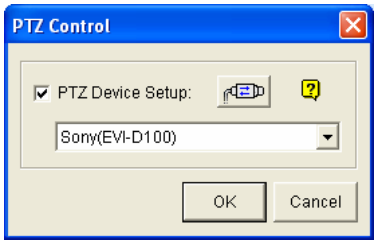


Figure 1-74

5. For **an IP camera**, select the brand name from the drop-down list and click **OK**.
6. For **an analog camera**:

A、 Select the brand name from the drop-down list, click the button.

B、 Select **Active**. Note that without this step the PTZ camera will not be added to the system.

C、 Click **OK**.

PTZ Control Panel

After the PTZ cameras are added to the system, you should now see the **PTZ Control** button on the screen. Click the button to bring out the on-screen control panel, shown as follows:

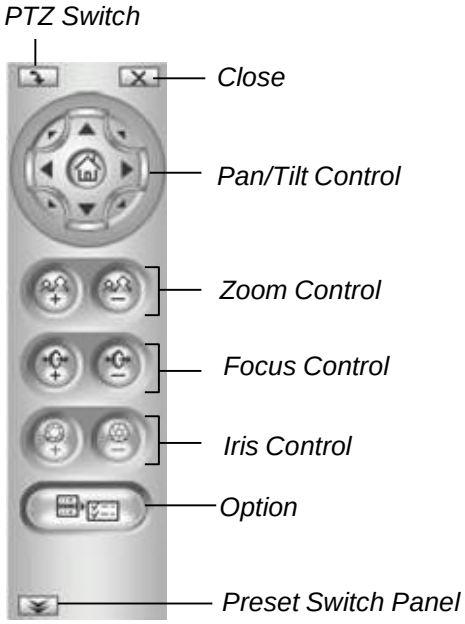


Figure 1-75

- **PTZ Switch:** Changes the PTZ model to be controlled.
- **Close:** Exits the control panel.
- **Pan/Tilt Control:** Allows the PTZ to pan and tilt to any angle.
- **Zoom Control:** Allows the PTZ to zoom in or out.
- **Focus Control:** Adjusts the camera focus.
- **Iris Control:** Adjusts the camera iris. The iris Control buttons are only available for -IP Speed Dome.
- **Option:** Moves the PTZ to a preset point by clicking the preset number. Functions included in the Option may be different in terms of PTZ models. Consult the manual of the connected PTZ model.
- **Preset Switch Panel:** You can also enter a preset number using the onscreen keypad displayed.

For the supported PTZ models, see *Appendix B*.

1.11.1 Mapping PTZ Cameras

This option assigns a PTZ camera to its corresponding camera channel for either the local or the remote applications. You must first make sure **PTZ Device Setup** in the PTZ Control section of the System Configure dialog box is selected.

⌘ For local applications, see *Auto Switching PTZ Control Panels* and *PTZ Automation* later.

⌘ For remote applications, this option will let you control PTZ cameras through the WebCam or Center V2 server.

1. Click the **Configure** button (No.14, Figure 1-2), point to **Accessories**, select **PTZ Device** and select **Camera Mapping PTZ Dome**. This dialog box appears.

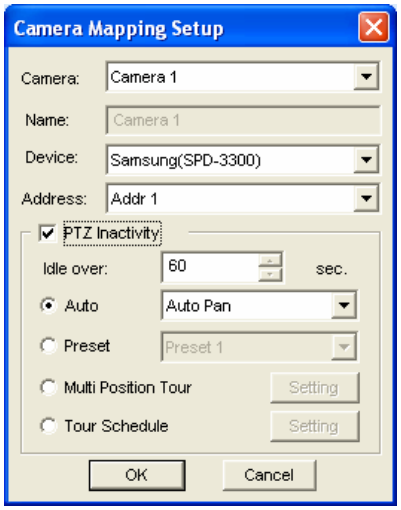


Figure 1-76 *Camera Mapping Setup*

2. Select a camera channel from the **Camera** drop-down list.
3. Select the PTZ model connected to the selected channel from the **Device** drop-down list.
4. If you have two identical PTZ cameras set in the system, you may use the **Address** drop-down list to choose the one with the correct address. Up to 64 addresses can be supported.
5. For the PTZ Inactivity settings, see *PTZ Idle Protection* later.
6. Click **OK** to apply the settings.

1.11.2 PTZ Idle Protection

When the PTZ remains stationary for a certain time, the PTZ can automatically activate the scan mode, move to the designated preset point, or start the preset tour.

1. In the Camera Mapping Setup dialog box (Figure 1-76), select **PTZ Inactivity**.
2. Set the idle time after which to start the protection mode.
3. Select **Auto**, **Preset**, **Multi Position Tour** or **Tour Schedule** as protection mode.

Setting Multi Position Tour

You can create a PTZ tour with up to 64 preset points. Note the number of preset points depends on your PTZ capacity.

1. Select **Multi Position Tour** on the Camera Mapping Setup dialog box (Figure 1-76), and click the **Setting** button. This dialog box appears.

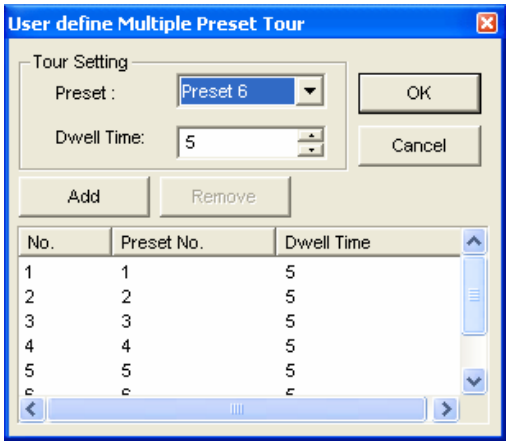


Figure 1-77

2. Select a **Preset** as a start point.
3. Set the **Dwell Time** that the PTZ will remain in a preset.
4. Click **Add** and repeat Steps 2-3 to build more points in the tour.

Setting Tour Schedule

When the PTZ camera remains stationary for a certain time, the camera will start the defined behaviors, such as activating the auto pan or returning the designated preset, in the defined time frames.

1. Select **Tour Schedule** on the Camera Mapping Setup dialog box (Figure 1-76), and click the **Setting** button. This dialog box appears.

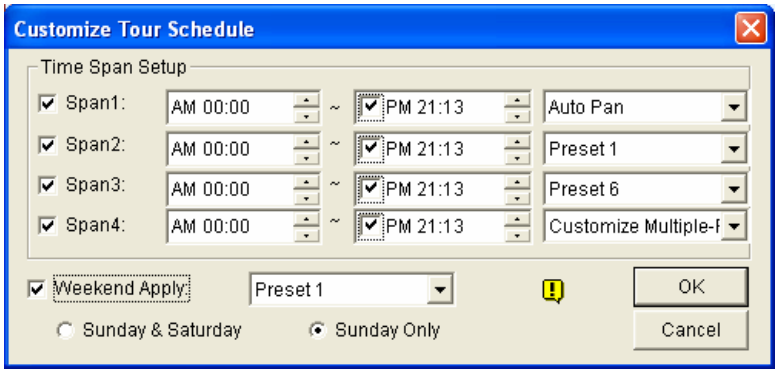


Figure 1-78

2. Select **Span 1**, specify a period of time, and select a camera behavior to be activated during the defined time period.
3. Set another span.
4. If you want to apply a different setting to weekends, select **Weekend Apply** and select a camera behavior. And define whether the weekend includes Saturday or not.
5. Click **OK** to apply the settings.

Note: It is required to set more than one span so that a specified camera behavior will only run in the defined time frame. Otherwise, you can select the **Auto**, **Preset** or **Multi Position Tour** option (see Figure 1-76) to configure the idle protection.

1.11.3 Auto Switching PTZ Control Panels

The function allows the corresponding PTZ control panels to be called up automatically when you switch to different PTZ camera screens. To enable the function, follow the steps below:

1. Click the **Configure** button (No. 14, Figure 1-2), point to **Accessories**, select **PTZ Device**, and then select **Auto PTZ Panel Switch**. The Camera Mapping Setup dialog box appears.
2. Select the corresponding camera channel, device model and hardware address for each PTZ camera. For details, see *Mapping PTZ Camera* earlier.
3. Click **OK**. When you change the channel, the corresponding PTZ control panel will appear on the screen.

1.11.4 PTZ Automation

Other than the PTZ control panel, you can display a Visual PTZ Control Panel on the image.

Figure 1-79

1. To control the PTZ, you must map one channel to the PTZ camera first. For details, see *Mapping PTZ Cameras* earlier in this chapter.
2. To access the Visual PTZ Control Panel click on the desired **Camera Name** on the top left corner of every channel, and select **PTZ Automation**. A separate PTZ control window appears.
3. To change the panel settings, click the green **PTZ** button on the top left corner of the PTZ control window to have these options:

   [PTZ Control Type]

   ④ **Fixed Direction Move:** In this mode, the dome view can only be moved to the eight directions (north, south, east, west, northeast, northwest, southeast and southwest). To move the camera view, click and hold on to the dotted red line further from the panel. The round panel appears when moving the mouse to the live view.

   ④ **Random Move:** In this mode, you can move the camera view to any direction. Click any place on the live view for the panel to appear, and right-click for the panel to hide. To move the camera view, click and hold on to a desired direction. Click further for the camera view to move faster.

   ④ **Center Move:** In this mode, you can zoom in and out using the mouse scroll or by drawing a block directly on the live view.

Note: The **Center Move** mode is only for -SD220.

- **Transparency:** Adjusts the transparency level of the panel. Ten levels range from 10% (fully transparent) to 100% (fully opaque).

1.12 Digital PTZ Control

In non-PTZ cameras, the Digital PTZ (DPTZ) function allows you to simulate the PTZ movement on the screen.

1. Right-click the live view, find **Camera Name** and select **Digital PTZ**. The **Visual Automation View** window for DPTZ control appears.

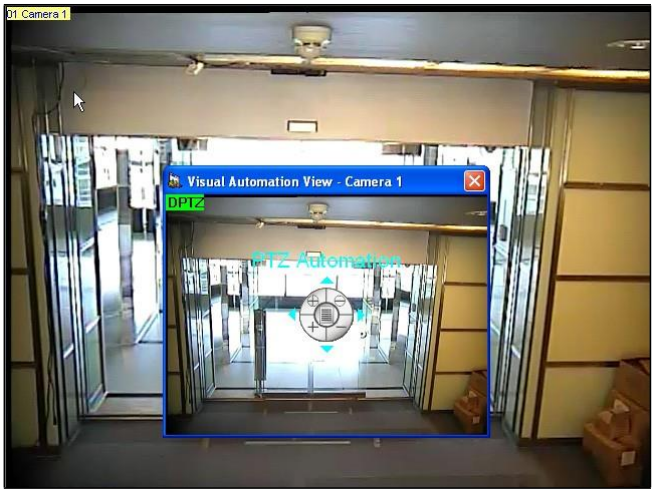


Figure 1-80

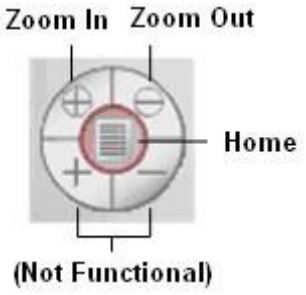


Figure 1-81

2. To zoom in / out, click the corresponding buttons or use the mouse scroll. To bring the Visual Automation View back to its default image, click **Home**.

3. To pan and tilt the Visual Automation View, zoom in on the image first, and then click and hold the arrow. The arrow appears when you place the cursor in one of the eight directions, i.e. up, down, left, right, left up, left down, right up and right down.

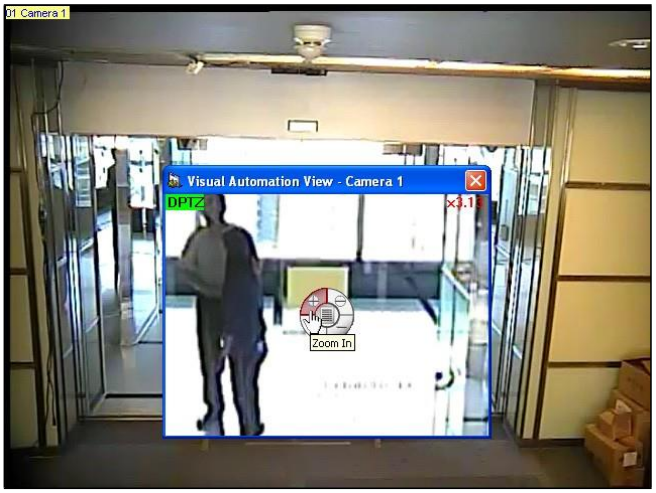


Figure 1-82 *Visual Automation View (zoom-in function applied)*

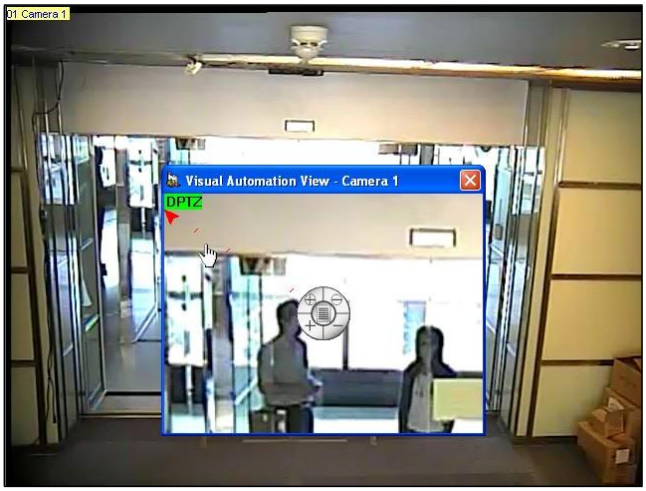


Figure 1-83 *Visual Automation View*
(tilt function applied by holding the arrow in the upper left corner)

4. To adjust the transparency level of the Control Panel, click the green **DPTZ** button on the top left corner of the window and select **Transparency**. Ten levels range from 10% (fully transparent) to 100% (fully opaque).

Note: The functions of Focus In / Out and the speed level are not supported in Digital PTZ.

1.13 Pop-up Live Video

The live video can pop up immediately for alert whenever motion detection and alarm occurs. To set up, click the **Configure** button (No.14, Figure 1-2), point to **Video Analysis**, and then select **Camera Popup Setting**. This brings up the following Camera Popup Setting dialog box.

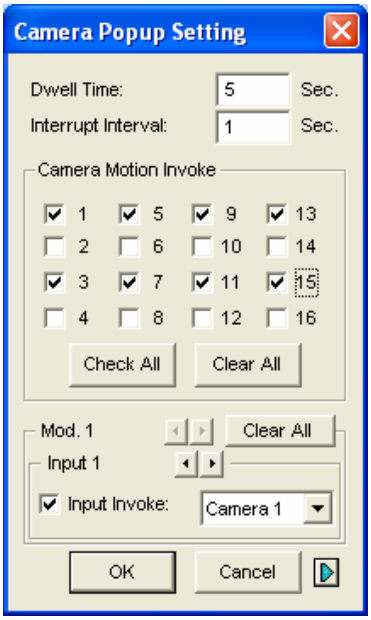


Figure 1-84

④ **Dwell Time:** Specify the amount of time a pop-up live video to remain in the foreground.

④ **Interrupt Interval:** Specify the interval between live video pop-ups. This feature is useful when several cameras are activated for a pop-up alert at the same time.

④ **Camera Motion Invoke:** Choose which camera you wish to have auto pop-up upon motion detection.

④ **Input Invoke:** Select an input module and number using arrow buttons, select this option and assign a camera to the input device. Whenever the input is triggered, the live video of the assigned camera will pop up.

④ **The Arrow Button:** The pop-up live videos appear on the screen when triggered events occur. If the DSP Spot Monitor function is enabled, you can select if pop-up live videos appear on the system screen, spot monitor or both. For details on DSP Spot Monitor Controller, see *Spot Monitor Controller* in Chapter 11.

Note: You can use the **Mask Filter** function in the Camera Configure dialog box (Figure 1-8) to mask off certain areas of the camera image that you don't want to detect motion.

1.14 Video Noise Solutions

The system provides these solutions for video/audio noise:

- **Noise Tolerance** for motion detection and advanced motion detection
- **Noise Detection to Reduce File Size** for round-the-clock recording
- **Noise Filter** to filter out video and audio noise

1.14.1 Noise Tolerance

Designed for motion detection, the noise tolerance feature reduces false alarms and unwanted recordings caused by weather or light changes. The level of noise tolerance can be adjusted.

Note: The noise tolerance function will not change video quality.

Setting Up for Motion Detection

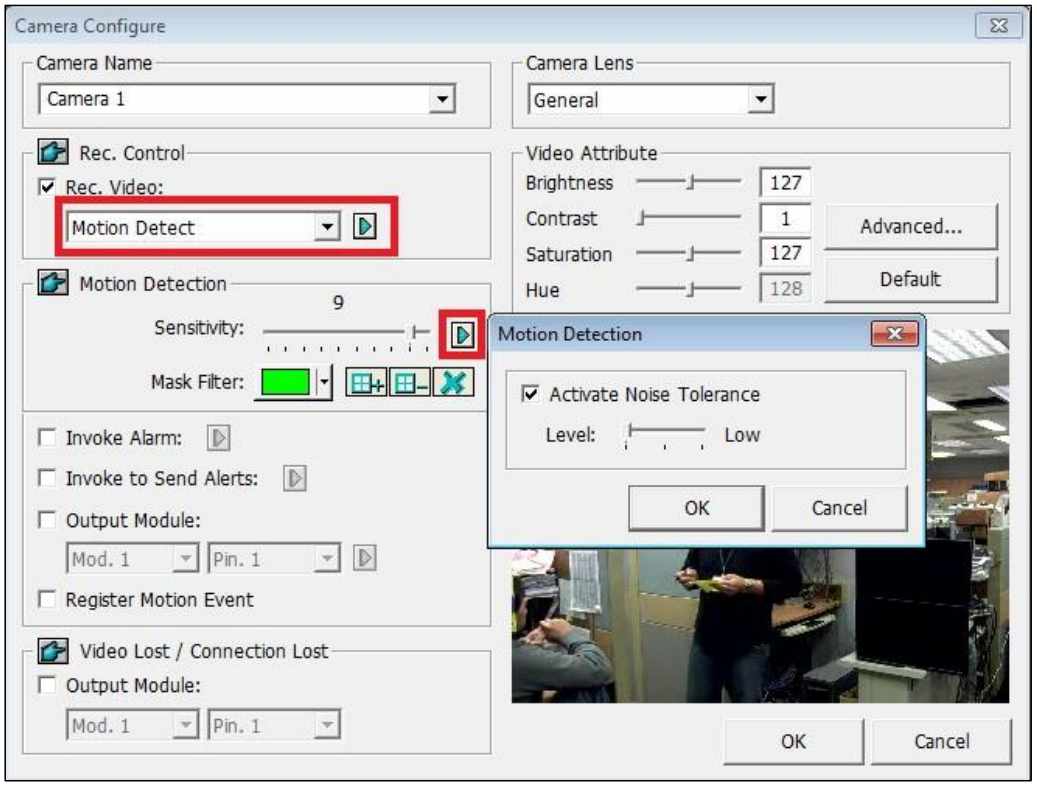


Figure 1-85

1. Click the **Configure** button (No. 14, Figure 1-2), point to **System Configure**, and select **Camera Configure**. A dialog box appears.
2. To set the recording mode to motion detection, enable **Rec. Video**, and select **Motion Detect** from the drop-down list.
3. To enable noise tolerance, click the right-arrow button next to **Sensitivity** in the Motion Detect section. The Motion Detection Setup dialog box appears.
4. Select **Activate Noise Tolerance** and adjust tolerance level. The higher the level, the more tolerant the system is to video noise. If your surveillance area may produce much video noise, set the level to High. Conversely, set the level to Low if the surveillance area may produce less video noise.
5. Click **OK** to save the settings.

Setting Up for Advanced Motion Detection

For details, see *Advanced Motion Detection* in chapter 3.

1.14.2 Noise Detection to Reduce File Size

Designed for the round-the-clock recording, the Noise Detection feature can automatically reduce recording size on video noise conditions, and restore normal recording size when the disturbing conditions are over.

1. Click the **Configure** button (No. 14, Figure 1-2), point to **System Configure**, and select **Camera Configure**. A dialog box appears.
2. To set the recording mode to Round-the-Clock, enable **Rec Video** and select **Round-the-clock** from the drop-down list.
3. Select **Apply Advanced Codec Setting** and click the button. This dialog box appears.

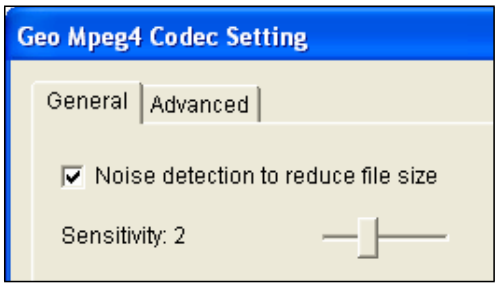


Figure 1-86

4. Select **Noise detection to reduce file size** and adjust the **Sensitivity** level. The higher the value, the more sensitive the system is to video noise.
5. Click **Apply**.

When the option is selected and video noise conditions are detected, you can see the icon overlaid on the right-bottom corner of recorded videos. So you can easily distinguish the normal- size segment from reduced-size segment. Note the icon does not appear on live video.

Note: You can also use this function when the recording mode is set to Motion Detection.

1.14.3 Noise Filter

The Noise Filter function can remove video and audio noise from live view. The video denoising can reduce file size and improve image quality, while the audio denoising can maximize the sound quality.

Filtering Out Video Noise

1. Click the **Configure** button (No. 14, Figure 1-2), point to **Video Analysis** and select **Video Lowpass Filter Setting**. This dialog box appears.

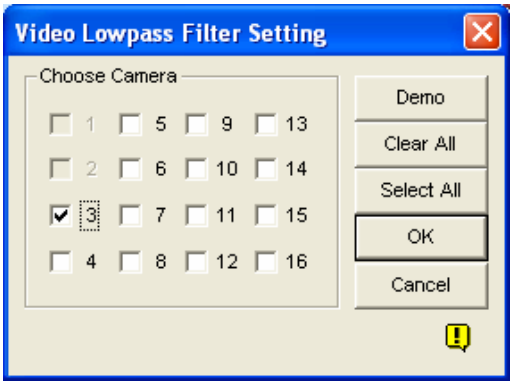


Figure 1-87

2. Select the desired channels to be filtered out video noises, and click **OK**. The video noises from the selected channels are reduced, and file sizes are decreased too.

Filtering Out Audio Noise

1. Click the **Configure** button (No. 14, Figure 1-2), point to **A/V Setting**, and select **Audio Settings**. A dialog box appears.
2. Select the desired channels to be filtered out audio noise, select **Wave Out De-Noise**, and click **OK**. The audio noises of the selected channels are reduced.

1.15 Picture-in-Picture View

With the Picture in Picture (PIP) view, you can crop the video to get a close-up view or zoom in on the video. This function is useful for megapixel resolution that provides clear and detailed images of the surveillance area.

1. Click the desired camera name and select **PIP View**.
2. The screen automatically switches to one division, and an inset window of the camera view appears in the bottom right corner.

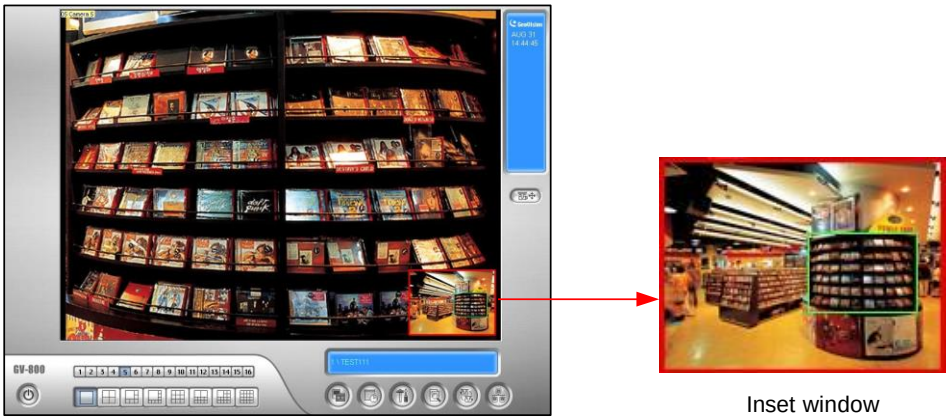


Figure 1-88

3. Double-click the inset window. A hand icon appears.
4. Click the inset window. A navigation box appears.

Figure 1-89

5. Move the navigation box around in the inset window to have a close-up view of the selected area.
6. To adjust the navigation box size, move the cursor to any of the box corners, enlarge or diminish the box.
7. To change the frame color of the navigation box, right-click the image, select **Mega Pixel Setting**, and select **Set Color of Focus Area**.
8. To exit the PIP view, click the camera name and click **PIP View** again.

1.16 Picture-and-Picture View

With the Picture and Picture (PAP) view, you can create a split video effect with multiple close-up views on the image. A total of 7 close-up views can be defined. This function is useful for megapixel resolution that provides clear, detailed images of the surveillance area.

1. Click the desired camera name on the screen, and select **PAP View**.
2. The screen automatically switches to one division, and a row of three inset windows appears on the bottom of the screen.

Figure 1-90

3. Draw a navigation box on the image, and this selected area is immediately reflected in one inset window. Up to seven navigation boxes can be drawn on the image.
4. To adjust a navigation box size, move the cursor to any of the box corners, enlarge or diminish the box.
5. To move a navigation box to another area on the image, drag it to that area.
6. To change the frame color of the navigation box, right-click the image, select **Mega Pixel Setting** and click **Set Color of Focus Area**.
7. To hide the navigation box on the image, right-click the image, select **Mega Pixel Setting** and click **Display Focus Area of PAP Mode**.
8. To delete a navigation box, right-click the desired box, select **Focus Area of PAP Mode** and select **Delete**.
9. To exit the PAP view, click the camera name and select **PAP View** again.
10. To add another navigation box when less than seven navigation boxes are drawn, click the camera name, select **PAP View** to enter, right-click the image, select **Mega Pixel Setting**, and then select **Enable Add-Focus-Area-Mode**.

1.17 Shortcuts

You can create up to 20 shortcuts on the main screen to a program or file.

1. Run **Fast Backup & Restore Main System** from the Windows Start menu. The Fast Backup & Restore MultiCam System window appears.
2. Click the **Customize Logo and Button** button, select **DVR**, and then select **User Define Setting**. This dialog box appears.

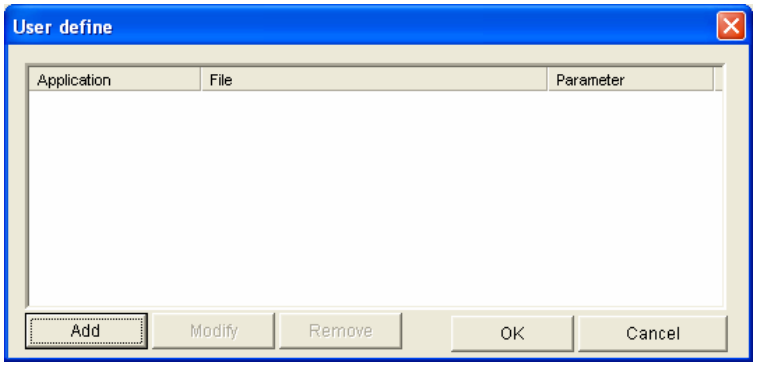


Figure 1-91

3. Click the **Add** button. This dialog box appears.

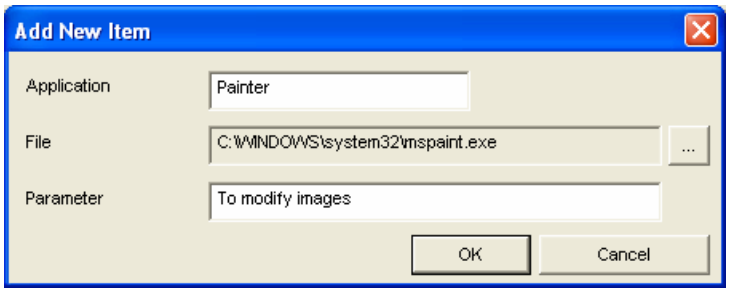


Figure 1-92

- ④ **Application:** Names the desired application to be pointed to.
- ④ **File:** Assigns the path to the desired application.
- ④ **Parameter:** Sets the command information for the application.

4. Click **OK** to save all the configurations.
5. Run the Main System. The shortcut button appears.

1.18 Touch Screen Support

The -System offers three types of control panels with touch screen support: PTZ Control Panel, I/O Control Panel and Touch Screen Panel.

1.18.1 PTZ and I/O Control Panel

This feature gives you the option of a large PTZ and I/O control panel with touch screen support. To open the panel, click the **Configure** button (No. 14, Figure 1-2), point to **Accessories**, select **PTZ Device**, select **PTZ/IO Panel**, and select **Large**.

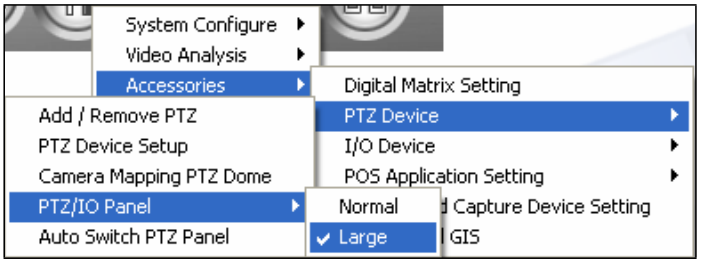


Figure 1-93

1.18.2 Touch Screen Panel

The touch screen panel allows you to switch to ViewLog and full screen by the touch of a finger. To open the panel, follow the steps below:

1. Click the **Configure** button (No. 14, Figure 1-2), point to **Tools**, select **Tool Kit**, point to **Touch Screen Panel** and then select **Panel Setup** to display the following window.

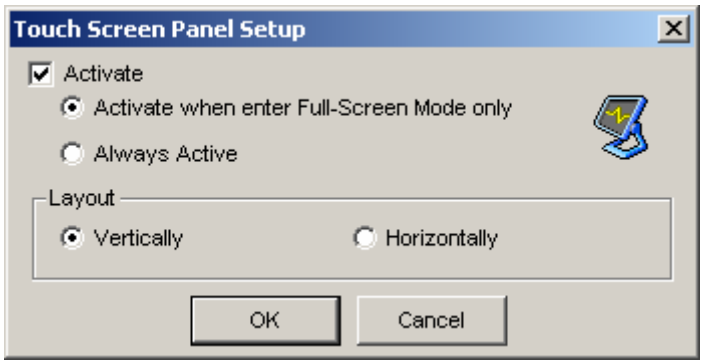


Figure 1-94

[Activate]

④ **Activate when enter Full-Screen Mode only:** Launches automatically the panel when the full screen view is applied.

④ **Always Active:** Always displays the panel on the screen.

[Layout] Choose a vertical or horizontal panel.

2. Click **OK** to save the above settings.
3. An information window indicating date, time, and storage space will appear at the upper left corner of the screen. Right-click it to open the touch panel as shown below.

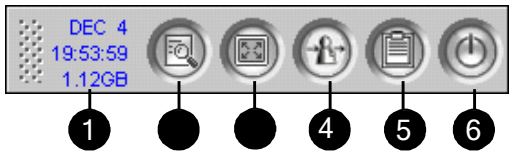


Figure 1-95

No.	Name	Description
1	Indicator	Indicates date, time and storage space.
2	ViewLog	Opens the ViewLog.
3	Full Screen	Switches to a full screen.
4	Login / Change User	Switches users to log in the -System.
5	System Log	Opens the System Log.
6	Close MultiCam	Closes the -System.

Note: You can move the touch screen panel anywhere on the screen by dragging it.

1.19 System Tools

1.19.1 Hard Disk Calculator

Before actual recording, the Hard Disk Calculator allows you to know the required hard disk space and frame size for different types of codec and quality.

1. Click the **Configure** button (No. 14, Figure 1-2), point to **A/V Setting**, select **Video Attributes**, and then click **Advanced**. The Advanced Video Attributes dialog box appears.
2. Click the **HDD Calculator** button at the right bottom. The HDD Calculator dialog box appears.

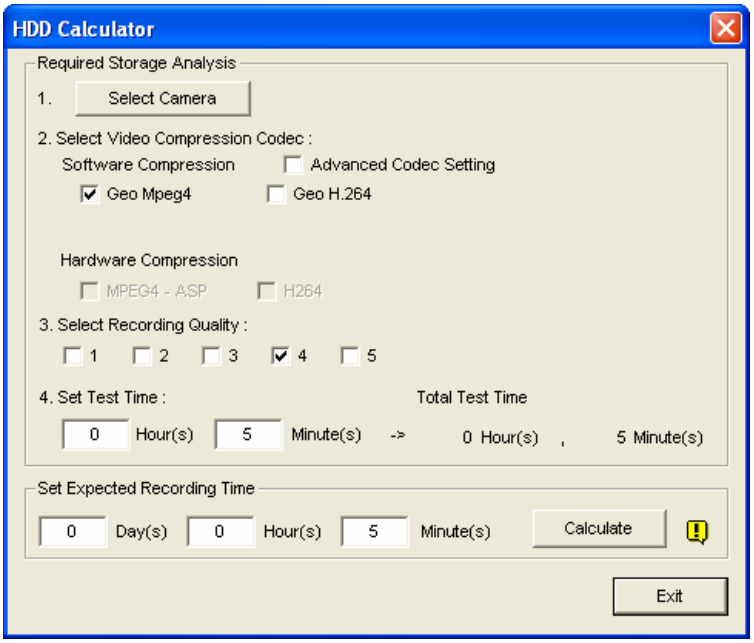


Figure 1-96

④ **Select Camera:** Select cameras to be used for recording.

④ **Select Video Compression Codec:** Check the desired codec(s) to be used for recording. You can choose more than one codec to compare their performance.

- **Software Compression:** Check the desired codec(s) to be used for recording. You can choose more than one codec for performance comparison. This option appears dimmed when -3008 or -4008 is installed.
- **Hardware Compression:** Check the desired codec(s) to be used for recording. This option is available when -3008 or -4008 is installed.

④ **Select Recording Quality:** Check the desired quality value(s) for recording. You can choose more than one quality value for comparison.

④ **Set Test Time:** The system will process a real-time test recording based on the time you set. For example, if you enter 24 hours here, it will take more than one day to do the test recording. So avoid entering the longer test time to save you time.

④ **Set Expected Recording Time:** Enter the time you wish for recording.

3. Click the **Calculate** tab to see the result.

Note:

1. A calculation difference by ± 5 % from actual disk usage is expected.
2. The video attribute settings will effect the hard disk calculation.
3. This function is not available to the IP cameras.

1.19.2 Colorful Mode

You can enhance the coloring of live video to have more vivid and saturated images. Note this function does not affect the original files.

For the users of -600A, -600B, -600(S), -650A, -650B, -650(S), -800A, -800B, -800(S), -804A, -900A, -4008, -4008A, -5016 or -SDI-204 Card:

1. Click the **Configure** button (No.14, Figure 1-2), select **System Configure**, select **General Setting**, select **Apply Directdraw Scale** in the Display dialog box, and restart the Main System.
2. Click the **Configure** button, select **Tools**, select **DirectDraw Configuration** and select **Use Colorful Mode.** Then restart the Main System for the mode to take effect.

For the users of -1120, -1120A, -1120B, -1240, -1240A, -1240B, -1480, -1480A -1480B,or -3008 Card:

1. Click the **Configure** button (No.14, Figure 1-2), select **System Configure**, select **General Setting**, select **Apply Directdraw Scale** in the Display dialog box, and restart the Main System.
2. Click the **Configure** button, select **Tools**, select **DirectDraw Configuration** and select **Use Colorful Mode**. Then restart the Main System.
3. Click the **Configure** button, select **A/V Setting**, clear the selection of **DSP Overlay**, and restart the Main System for the colorful mode to take effect.

Note: The Colorful Mode can be applied to any connected channels of IP devices directly by selecting **Use Colorful Mode** and then restarting the Main System.

1.19.3 Stopping Video Lost Watchdog

When the video signal is weak, the software watchdog will try to recover the lost video by restarting the system and even rebooting the computer. By default, the video lost watchdog is enabled. To disable this feature, click the **Configure** button (No. 14, Figure 1-2) , point to **Tools**, select **Video Signal Diagnostic**, and select **Disable Video Signal Weak Watchdog**.

Note: This function is not available in -NVR System.

1.19.4 Deactivating Video Lost Beep

To stop a beep noise when any of videos lost, click the **Configure** button (No. 14, Figure 1-2), point to **Tools**, select **Video Signal Diagnostic**, and select **Disable Video Lost Beep**.

1.19.5 Fast Key Lockup

If you wish not to use certain fast keys and do not want them to interfere with the keyboard use, you can disable the fast key functions.

1. Click the **Configure** button (No. 14, Figure 1-2), point to **Tools**, select **Tool Kit**, and then select **Fast Key Lock Setup**. This dialog box appears.

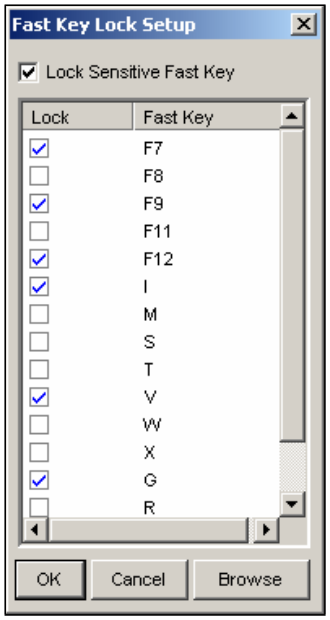


Figure 1-97

2. Check **Lock Sensitive Fast Key**, and check the fast keys you want to disable. To restore the fast keys, uncheck them again.
3. Click **OK** to apply your settings.

1.19.6 Fast Key Reference

This option lets you view the fast key windows of Main System and PTZ Control, giving you an instant reference. Click the **Configure** button (No. 14, Figure 1-2), point to **Tools**, select **Tool Kit**, and then select **Fast Key List** to display the fast key table of Main System. Click **Next** to display the table of PTZ Control.

1.19.7 Network Failure Detection

The Network Failure Detection function triggers an output device when the network connection between -System and the specified network host has failed. You can set a time interval, which specifies how often the -System will send a ping message to the network host to check if the connection is still active.

1. Click the **Configure** button, select **Tools** and click **Network failure detection**. This dialog appears.

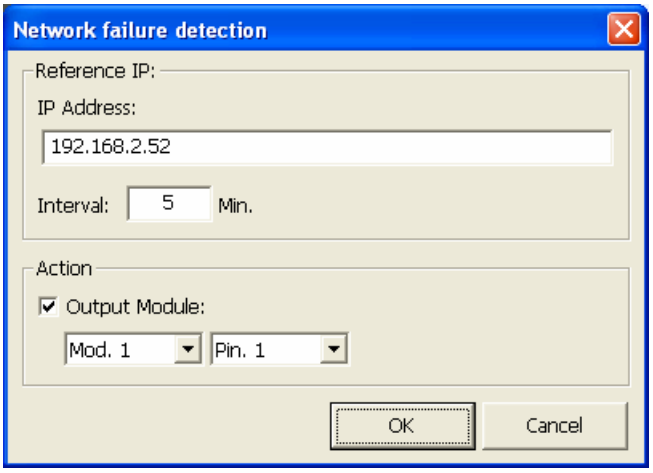


Figure 1-98

2. Under **IP Address**, type the IP address or domain name of the remote host.
3. Next to **Interval**, type the time interval between each ping in minutes ranging from 1 to 999. If the interval is 5 minutes, -System will ping the network host every 5 minutes.
4. Under Action, enable **Output Module** and select the output module and pin number.
5. Click **OK**.

The select output device will be triggered when the network host does not respond to -System's ping message.

1.19.8 Memory Limit

The -System can automatically warn you on high memory usage to prevent system instability. The memory monitoring and warning function requires your system to be **Windows XP SP1 or later**.

The memory limit of -System or Main System is as listed below:

- For users of 32-bit Windows, the memory limit is **1.7 GB**.
- For users of 64-bit Windows, the memory limit is **1.7 GB with 2 GB RAM** and **3 GB with 4 GB RAM**.

When the memory usage of the -System exceeds the limit, the warning message will pop up. The system can become unstable if the high memory persists. To reduce memory usage, you can close one or more of these applications: connection to IP video devices, Video Analysis, Advanced Video Analysis and Pre-Record by Memory. The system will check the memory usage of the -system every 60 minutes.

To disable the memory warning function, click the **Configure** button (No. 14, Figure 1-2), click **Tools**, select **Memory Usage**, select **Hide Warning Message**, and click **OK**.

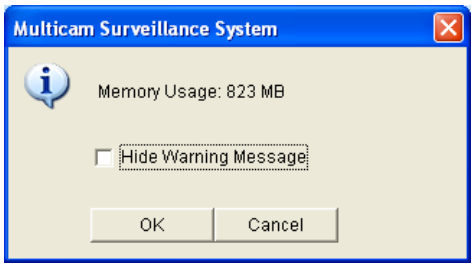


Figure 1-99

1.19.9 Version Information

To know which version of -System you have, click the **Configure** button (No. 14, Figure 1-2), point to **Tools**, and then select **Version Information**.

Chapter 2

Hybrid and NVR Solution 116

2.1 Sting Alarm IP Video Products..... 116

2.2 Dongle Requirement..... 117

2.3 Hybrid Solution Description 118

2.4 NVR Solution Description 119

2.5 IP Channel Setup 120

2.5.1 Adding Cameras Manually..... 121

2.5.2 Scanning Camera 123

2.5.3 Automatic Setup..... 124

2.5.4 Customizing IP Camera Settings 125

2.6 PTZ IP Camera 127

2.7 RTSP Connection 128

2.8 ONVIF & PSIA Connection 130

2.8.1 ONVIF Connection..... 12530

2.8.2 PSIA Connection..... 12532

2.9 Camera Mapping Using IP Device Utility..... 133

2.10 Economic Mode 135

2.11 On Demand Display..... 138

CHAPTER 2

Hybrid and NVR Solution

To implement IP video surveillance, Sting Alarm provides the two solutions:

- **Hybrid Solution:** Integrates analog videos with digital videos from IP video devices.
- **NVR Solution:** A software-based system -NVR without requiring a video capture card.

Both Hybrid and NVR Solutions come with 32 free IP channels when connecting to Sting Alarm IP video devices.

Sting Alarm's Hybrid and NVR solutions support not only Sting Alarm's own IP video products but also products from other leading manufacturers. For the supported IP devices, refer to the *Supported IP Camera List* at http://www.Sting Alarm.com.tw/english/4_21.asp.

Note: -250 Card does not support the Hybrid solution.

2.1 Sting Alarm IP Video Products

Sting Alarm offers a comprehensive line of IP video products:

- **-IP Camera:** -IPCAM H.264 series cameras, including Box Camera, Mini Fixed Dome, Bullet Camera, PTZ Camera, PT Camera, Vandal Proof IP Dome, Fixed IP Dome, Cube Camera and Fisheye Camera.
- **-Video Server:** Converts up to 1, 2 or 4 analog camera(s) into IP camera(s).
- **-Compact DVR:** Converts up to 4 or 8 analog cameras into IP cameras.
- **-NVR:** A complete software-based solution for IP video surveillance.

2.2 Dongle Requirement

To perform third-party IP devices with the Hybrid or NVR soltuion, you will need a NVR dongle to run the -System. There are two types of dongles: internal dongle with hardware watchdog function and external dongle.

- The dongle options include: 1, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32 IP channels.

It is required to install drivers from the Software DVD for the NVR dongle to work.

See *USB Dongle Required for IP Device Application* in *Appendix A.*

2.3 Hybrid Solution Description

1. **Specifications of the Hybrid solution.** The Hybrid solution integrates analog videos with digital videos from IP video devices with the limit of 32 channels in total. The Hybrid solution allows you to connect up to 32 IP channels from Sting Alarm IP devices for free.

   For example:

   Number of analog channels + up to 32 free IP channels <= 32 channels.

2. **Connection of third-party IP devices to -System.** To implement the Hybrid solution with third-party IP video devices, you will need a **NVR Dongle**.

   - The dongle options include: 1, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32 IP channel(s).

   In this case, the total number of channels for your Hybrid system is: Number of analog channels (+ up to 32 free IP channels) + Number of channels in your **NVR Dongle** <= 32 channels.

2.4 NVR Solution Description

1. **Specifications of the NVR solution:** The NVR solution supports up to 32 IP channels. It allows you to connect up to 32 IP channels from Sting Alarm IP devices for free.
2. **Connection of third-party IP devices to -NVR.** To implement the -NVR solution with third-party IP video devices, you need a **NVR Dongle**.
    - Dongle options include: 1, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32 IP channel(s).

2.5 IP Channel Setup

There are many ways to set up IP cameras in the system and the setup procedures may vary slightly among IP camera, video server and compact DVR. Click the **Configure** button (No. 14, Figure 1-2), select **System Configure**, select **Camera Install** and click **IP Camera Install**. This dialog box appears.

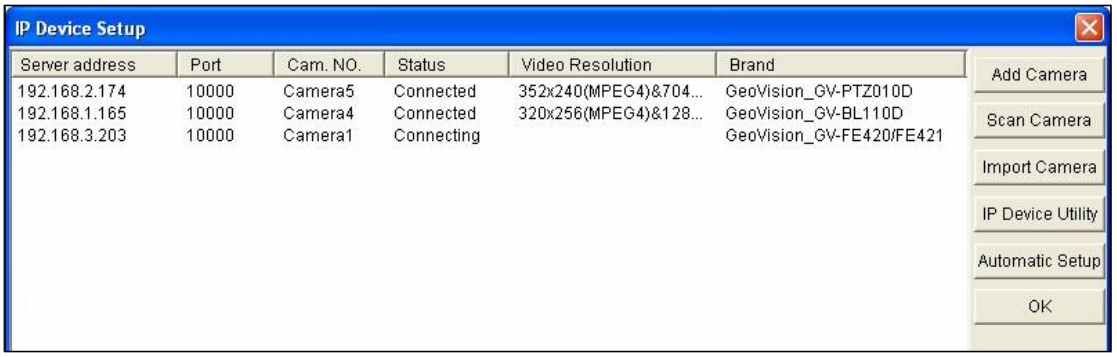


Figure 2-1

- ⌘ To automatically set up an IP camera, click **Scan Camera** to detect any IP cameras on the same LAN.
- ⌘ To manually set up an IP camera, click **Add Camera**.
- ⌘ To import IP cameras from the -IP Device Utility, click **Import Camera**.
- ⌘ To map IP devices through the IP Device Utility, click **IP Device Utility**.
- ⌘ To add all IP cameras within an IP address range, click **Automatic Setup**.

To see more details on importing and mapping cameras using -IP Device Utility, refer to C*amera Mapping Using -IP Device Utility* later in this chapter. For the other methods, refer to the sections below.

2.5.1 Adding Cameras Manually

An example of manual setup is described below.

1. Click **Add Camera**. This dialog box appears.

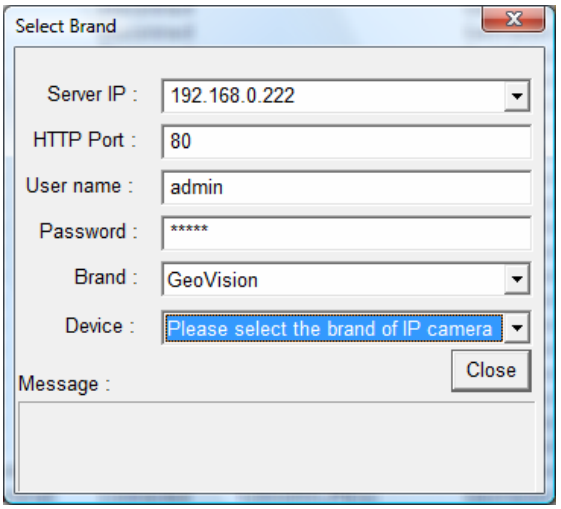


Figure 2-2

2. Type the IP address, username and password of the IP camera. Modify the default HTTP port 80 if necessary.
3. Select a camera brand and model name from the **Brand** and **Device** drop-down lists respectively. This dialog box appears.

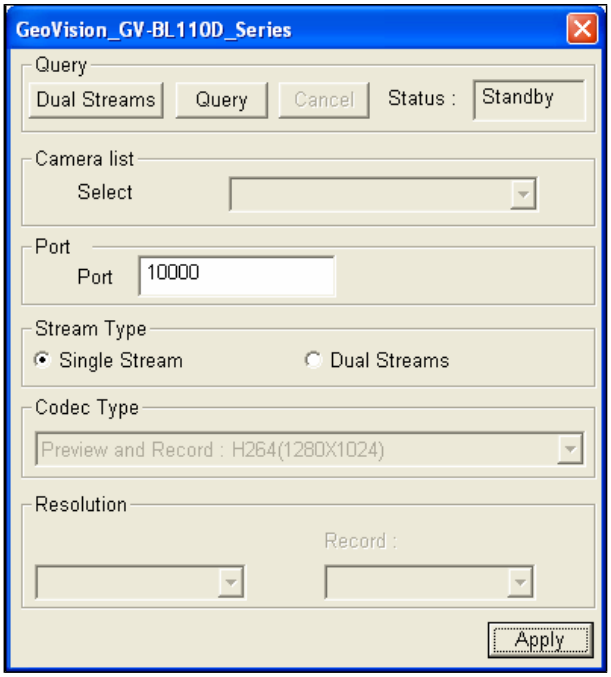


Figure 2-3

4. The options in the dialog box may vary depending on camera brands.
   - ④ **Dual Stream:** Use the default codec and resolution of the -IP camera. To see the default resolutions after the camera is added, refer to *Appendix I*.
   - ④ **Query:** Use the current codec and resolution setting on the -IP camera.
   - ④ **Camera list**: Select a camera number.
   - ④ **Port:** Video streaming port number.
   - ④ **Stream Type:** You may have the option of single or dual streaming depending on camera models.
   - ④ **Codec Type:** You may have different codec options depending on camera models. If the selected camera supports dual streaming, the preview codec and recording codec can be set differently.
   - ④ **Resolution:** You may select the different resolutions for preview and recording.
5. Click **Apply**. The IP camera is added to the list.
6. Right-click the camera and select **Display position** to map the IP camera to a channel on the -System.

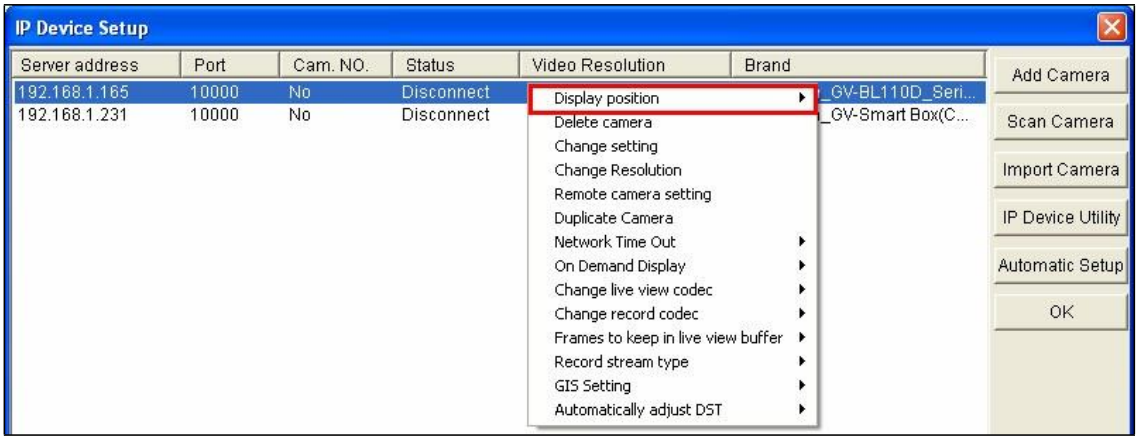


Figure 2-4

7. The Status column now should display "*Connected*". Click **OK**.

To customize camera settings such as codec and frame rate, right-click the camera to see the list of options. See *Customizing IP Camera Settings* section below for more details.

Tips: You can access the configuration interface of the connected IP device by right-clicking the IP device and selecting **Remote Camera Setting**.

2.5.2 Scanning Camera

You can add camera by scanning for cameras in the LAN.

1. Click **Scan Camera**. A dialog box appears.
2. Click the **Start Scan** button. IP devices detected are displayed.

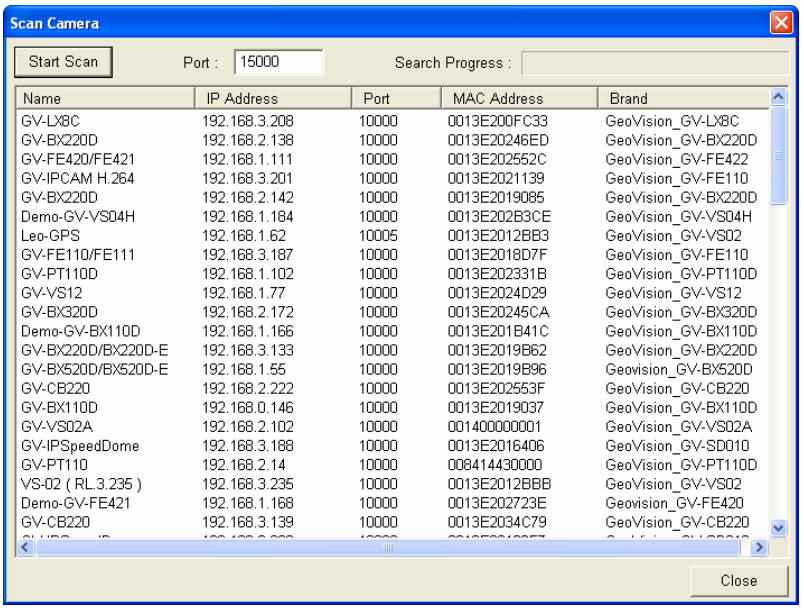


Figure 2-5

3. Double-click a device.
4. The username and password are set to **admin** by default. If the camera does not use the default settings, a dialog box will appear for you to type the correct username and password.
5. Follow steps 4-8 in the *Adding Cameras Manually* section above.

2.5.3 Automatic Setup

Using Automatic Setup, you can add all Sting Alarm and third-party IP cameras within an IP address range.

1. Click **Automatic Setup**. A dialog box appears.

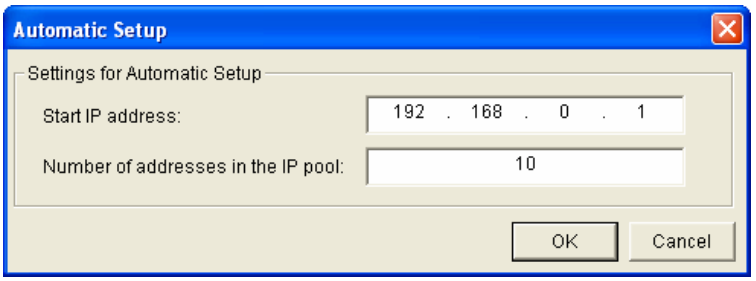


Figure 2-6

2. Type a **Starting IP address** and specify the **number of addresses in the IP pool** to include. In the case of the figure above, IP devices using IP address between 192.168.0.1 and 192.168.0.10 will be added.
3. Click **OK**.

-System will automatically try to establish connection with IP devices within the defined IP range. The username and password are set to **admin** by default. If the camera does not use the default settings, the status will be displayed as “Connecting.” To change the login settings, right-click the camera and click **Disconnect Camera**. Right-click the camera again and click **Change Setting** to modify the username and password.

2.5.4 Customizing IP Camera Settings

To configure IP camera settings such as frame rate, codec type and resolution, right-click the desired camera to see the following list of options:

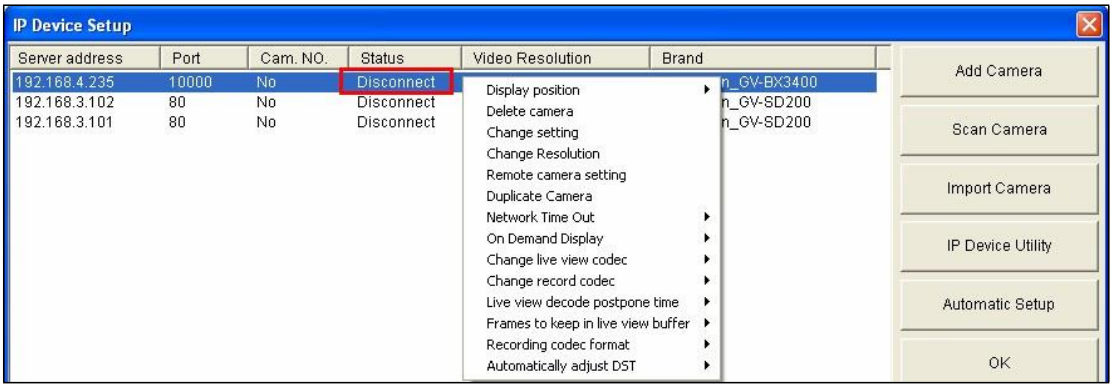


Figure 2-7

④ **Change Setting:** Changes the IP address, port number, username and password of the camera. Only available when the IP camera is disconnected.

④ **Change Resolution:** Changes the display ratio, live view resolution and record resolution.

④ **Remote Camera Setting:** Accesses the configuration interface of the connected IP device.

④ **Duplicate Camera:** Duplicates camera settings to quickly add multiple cameras of the same model. You can choose to use the same IP address but different port numbers or use the same port number but different IP addresses for each duplicated camera. Only available when the IP camera is disconnected.

④ **Network Time Out:** When network disconnection exceeds the specified time period, the camera status will be displayed as Connection Lost.

④ **On Demand Display:** Enables automatic adjustment of live view resolution. See the *On Demand Display* section later in this chapter for more details.

④ **Change Live View Codec:** Changes the live view codec.

④ **Change record codec:** Changes the recording codec.

④ **Live view decode postpone time:** Specifies the number of milliseconds to postpone live view decoding. When network connection with IP devices is unstable or when the time length between frames is not evenly distributed, postponing the live view decoding will make the video smoother.

④ **Frames to keep in live view buffer:** Specifies the number of frames to keep in the live view buffer. When CPU performance is insufficient, you can reduce the number of frames kept in buffer to achieve a real-time appearance by dropping frames. This setting does not affect the frame rate of the recorded videos.

④ **Recording codec format** Specifies whether to record in standard or Sting Alarm type of JPEG, MPEG4, H.264 codec.

④ **GIS Setting:** Records the video with the GPS data. To record the GPS data, remember to also enable the GIS function of the -System (Configure button < Accessories < Enable Local GIS).

④ **Automatically adjust DST:** If enabled, the time on the -IP device Web interface will be synchronized with the time of the -System when DST period starts or ends on the -System.

After a display position is assigned and the camera becomes connected, you can also access the following options:

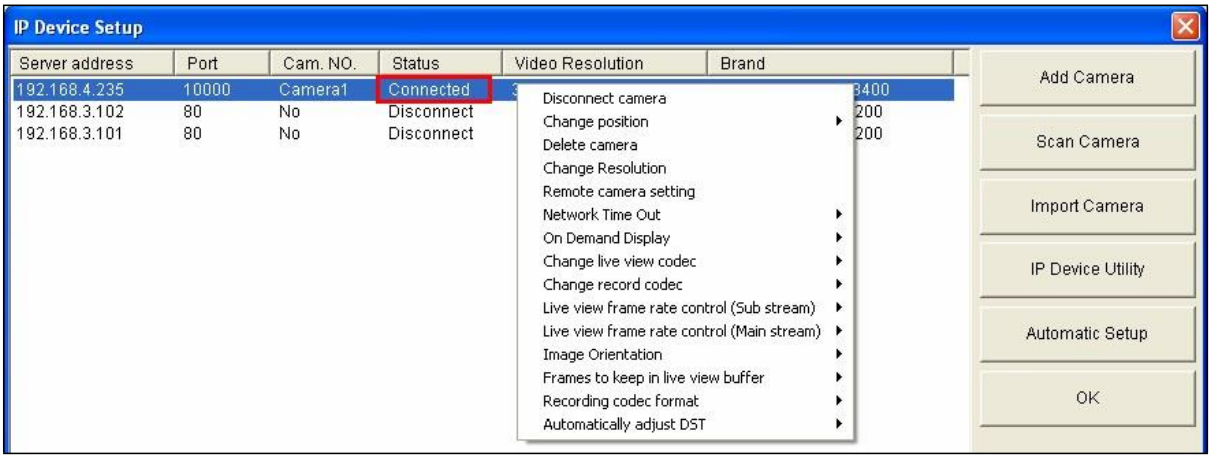


Figure 2-8

④ **Live-view frame rate control (Sub stream):** Sets the live view frame rate of the sub stream to help reduce the CPU usage. If you have set the live view codec to be **JPEG**, select the number of frames to allow in a second. If the live view codec selected is **MPEG4** or **H.264**, select one of the following options:

- **Maximum Live-view Frame Rate:** View the video at the maximum frame rate possible.
- **Live-view Key Frame only:** You can choose to view the key frames of the videos only instead of all frames on the live view. This option is related to the GOP setting of the IP camera. For example, if the GOP value is set to 30, there is only one key frame among 30 frames.

④ **Live-view frame rate control (Main stream):** Sets the live view frame rate of the main stream with higher resolution when On Demand function is enabled. Refer to *Live-view frame rate control* above to see the options available.

④ **Image Orientation:** You can adjust the image orientation by selecting **Normal**, **Horizontal Mirror**, **Vertical Flip** or **Rotate 180**.

Note:

1. Some options are not available for -Fisheye Cameras.
2. When CPU loading is high, selecting **Live-View Key Frame Only** can reduce CPU loading by jumping from key frame to key frame and dropping the non-key frames in between. This settings do not affect the frame rate of the recorded videos.

2.6 PTZ IP Camera

To set up the IP camera with PTZ functions, follow these steps:

1. To add the PTZ IP camera to the system, follow the steps in *Adding IP Video Sources* above.
2. To open the PTZ control panel and perform the PTZ functions, follow the steps in *PTZ Control* in Chapter 1.

2.7 RTSP Connection

You can add an IP camera to the -System by using the RTSP (Real Time Streaming Protocol) if this protocol is supported by your IP camera. This is useful to set up an IP camera which is not on the list of Supported IP Devices (see http://www.Sting Alarm.com.tw/english/4_21.asp).

Note: The RTSP is a protocol that allows you to access video streams by using the compatible media players like Windows Media Player or equivalent software like -System.

---

1. Click the **Configure** button (No.14, Figure 1-2), select **System Configure**, select **Camera Install** and click **IP Camera Install**.
2. Click the **Add Camera** button to manually add an IP camera. The Select Brand dialog box appears.
3. Type the IP address, username and password of the IP camera. Modify the default HTTP port if necessary.
4. Select **Protocol** from the **Brand** drop-down list.
5. Select the protocol that is supported by your IP camera from the **Device** drop-down list.

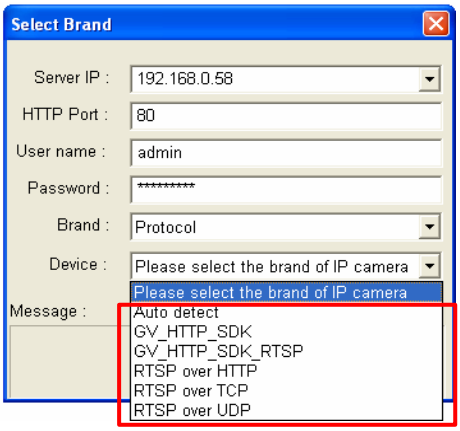


Figure 2-9

④ **_HTTP_SDK_RTSP:** This option is for Sting Alarm SDK users. The RTSP protocol uses a HTTP port for data streaming from the IP camera.

④ **RTSP over HTTP:** The RTSP protocol uses a HTTP port for data streaming from the IP camera.

④ **RTSP over TCP:** The RTSP protocol uses a TCP port for data streaming from the IP camera.

④ **RTSP over UDP:** The RTSP protocol uses an UDP port for data streaming from the IP camera.

6. On the RTSP Command dialog box, enter the RTSP link address. For the RTSP command, consult the documentation of your IP camera. For instance:
   - For an AXIS IP camera, enter RTSP://<IP of the IP camera>/<codec>/media.amp
   - For a HIKVISION IP camera, enter RTSP://username:password@<IP of the IP Camera>
7. Click **OK**. The IP camera is added to the list.

2.8 ONVIF & PSIA Connection

The -System is compatible with all other IP video devices using ONVIF and PSIA standards. The ONVIF (Open Network Video Interface Forum) specification and PSIA (Physical Security Interoperability Alliance) specification are global standards created to ensure network video products from different manufacturers are compatible with each other.

2.8.1 ONVIF Connection

-System supports dual streaming of IP cameras connected through ONVIF protocol. For each stream, you can set codec, resolution, maximum bit rate, maximum frame rate, image quality and GOV values.

To add and set up an IP camera through ONVIF protocol:

1. Click the **Configure** button (No.14, Figure 1-2), select **System Configure**, select **Camera Install**, and select **IP Camera Install**.
2. Click **Add Camera**. This dialog box appears.

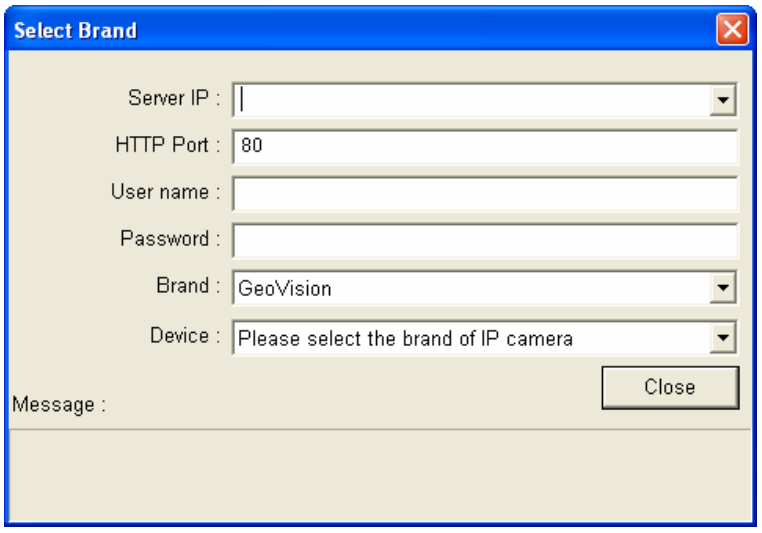


Figure 2-10

3. Type the **IP** address, **User name**, and **Password** of the camera.
4. For Brand, select **Protocol**; for Device, select **ONVIF**. A dialog box appears after the system confirms that the camera is ONVIF compatible.

5. To set the second stream if available, select Dual Stream for **Stream Type**.

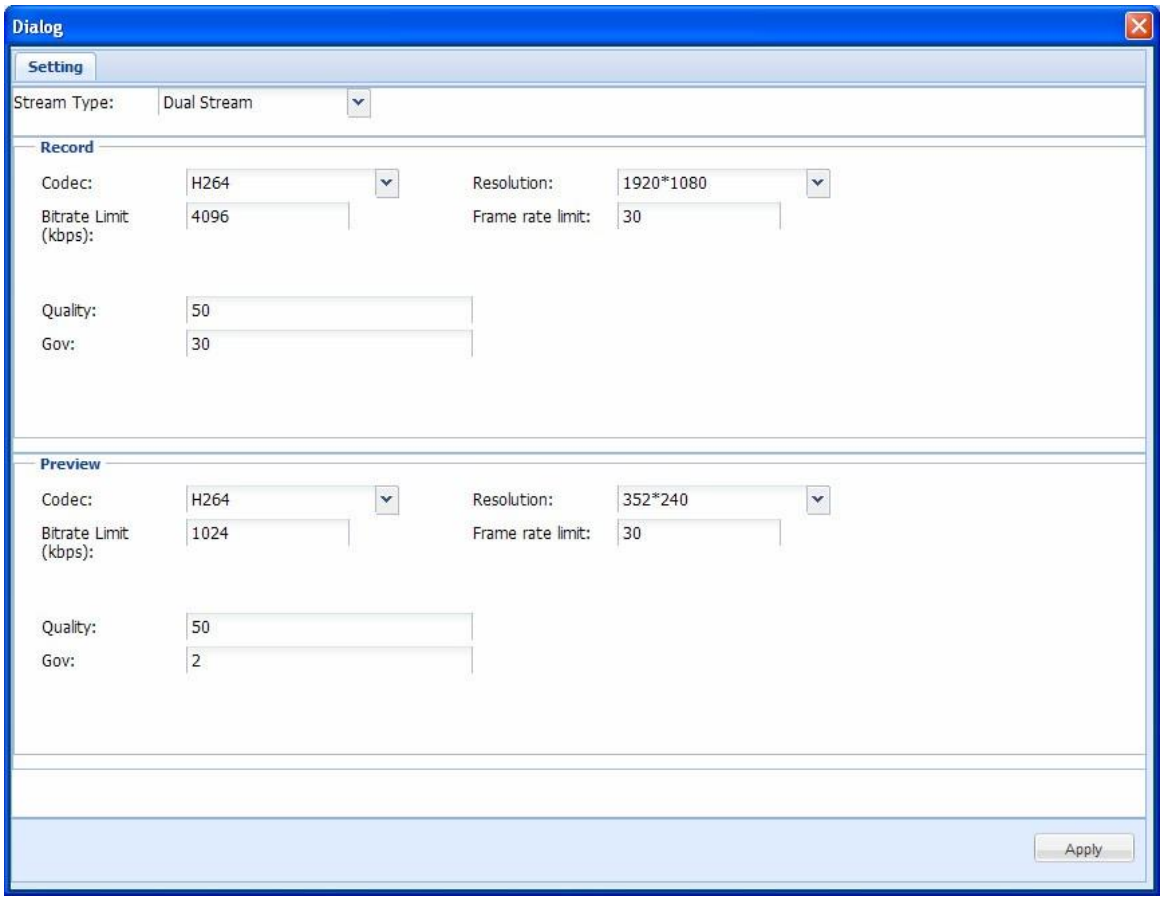


Figure 2-11

6. The following settings are available for each stream.

   - **Codec:** Select H.264 or JPEG.
   - **Resolution:** Set a resolution. The maximum resolution for stream 2 is limited to 800 x 600.
   - **Bitrate Limit:** The current bit rate setting of the IP device will be displayed. You can adjust the bit rate limit within the device's supported bit rate range if needed.
   - **Frame Rate Limit:** Set a maximum frame rate.
   - **Quality:** Adjust the image quality. The range of image quality varies for different brands.
   - **Gov:** Set the number of frames between each key frame. For example, a Gov of 10 means there will be 1 key frame every 10 frames.

7. Click **Apply**. The IP camera is now added to the camera list.

8. You can right-click the device in the camera list to access additional settings.

2.8.2 PSIA Connection

To connect to an IP device through PSIA protocol, follow the steps below.

1. Click the **Configure** button (No.14, Figure 1-2), select **System Configure**, select **Camera Install**, and select **IP Camera Install**.
2. Click **Add Camera**, and type the camera's **Server IP**, **Username**, and **Password**.
3. From the **Brand** drop-down list, select **Protocol**.
4. For Brand, select **Protocol**; for Device, select **PSIA**. A dialog box appears.

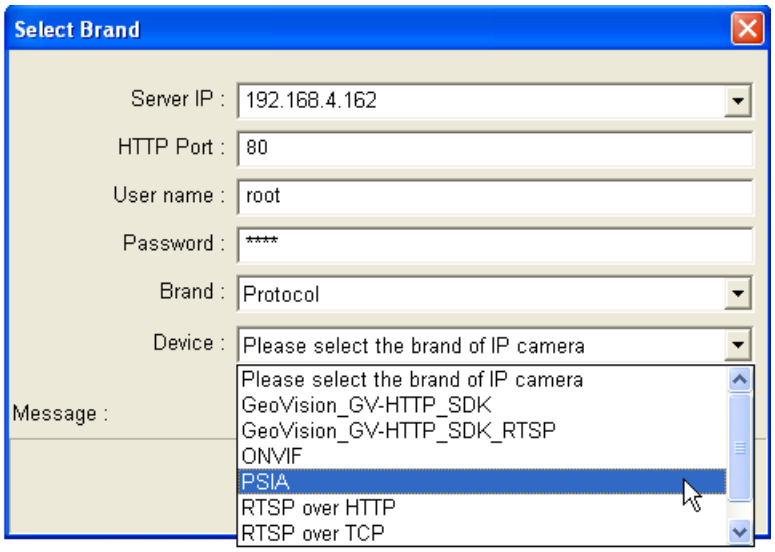


Figure 2-12

5. A dialog box appears after the system confirms that the camera is PSIA compatible. Click **Query**.
6. After the camera is located, click **Apply**.

2.9 Camera Mapping Using IP Device Utility

The IP Device Utility program can search and manage all the available IP devices on the same LAN, making it time-effective to map the connected IP cameras to channels. For convenient management, you can also save one or multiple sets of configurations and apply them according to your needs.

To set up multiple IP cameras using IP Device Utility:

1. Click the **Configure** button (No. 14, Figure 1-2), select **System Configure**, select **Camera Install**, and select **IP Camera Install**. The IP Device Setup dialog box appears.

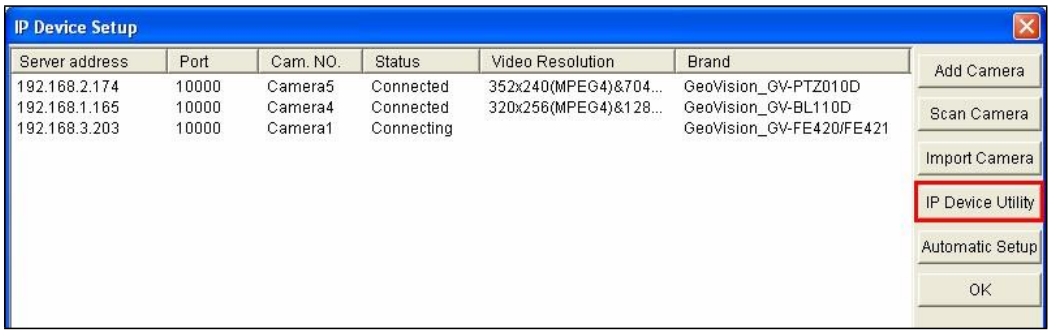


Figure 2-13

2. In the IP Device Setup dialog box, select **IP Device Utility**. This window appears. All the available IP cameras on the LAN are detected and listed in the window.

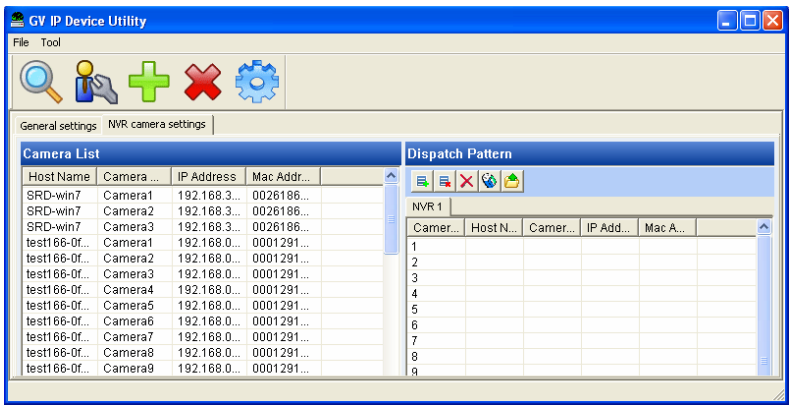


Figure 2-14

3. To map the desired IP camera to a channel, drag the IP camera from the **Camera List** to the desired channel number in the **Dispatch Pattern** section.

4. By default, the login username and password for the IP camera both are set to **admin**. If the added IP camera does not use the default settings, you need to right-click the IP camera in the **Dispatch Pattern** section and select **Login User Information** to modify its login information.

5. Repeat steps 3 and 4 to map more IP cameras.

6. To create another set of the IP camera mapping settings, click the **Add** button on the Dispatch Pattern toolbar. A new tab (NVR2) is created.

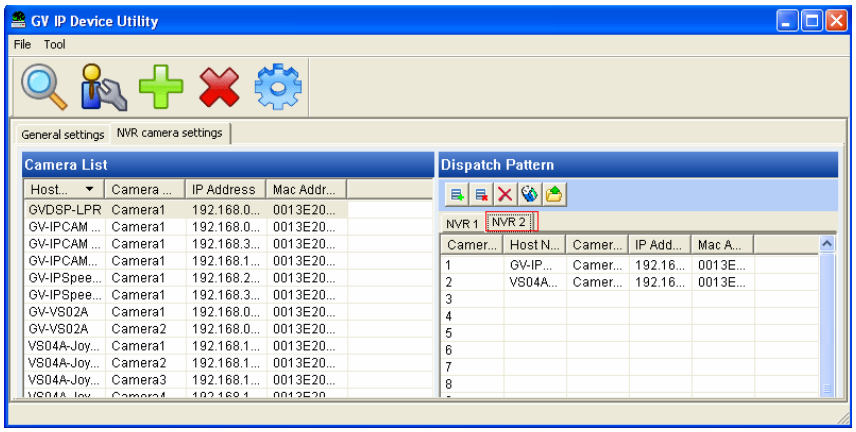


Figure 2-15

7. When you finish selecting the IP cameras, export the IP camera mapping settings.

   A. Select the tab of the IP camera mapping settings (NVR1, 2, 3,…) you want to apply and click the **Export** button on the Dispatch Pattern toolbar. The Save As dialog box appears.

   B. Specify the file name (.ipcd) and the storage path of the IP camera mapping settings.

   C. To export more sets of IP camera mapping settings, repeat the steps above.

8. Import the IP camera mapping settings into the -System.

   A. Close the **IP Device Utility** window, return to the IP Device Setup dialog box and select **Import Camera**.

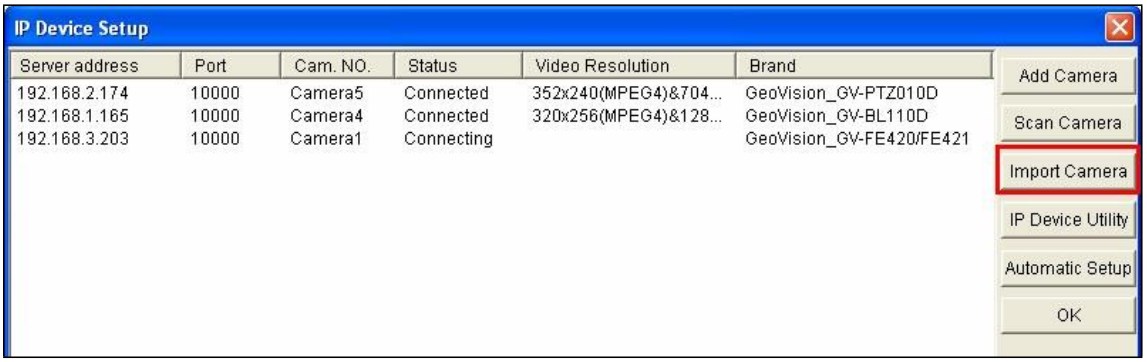


Figure 2-16

9. Locate the storage path of the IP camera mapping settings you want to import and click OK. The settings are updated to the -System.

2.10 Economic Mode

The economic mode helps you reduce the disk space needed to store videos from IP video devices. Once the economic mode is enabled, you can choose to record key frames only or at a lower frame rate when no motion is detected or when I/O devices are not triggered. This can significantly reduce the file size of the recorded events.

Note: The Economic Mode can only be applied to IP cameras.

To set up the economic mode:

1. Click the **Configure** button (No.14, Figure 1-2), select **System Configure**, and select **Camera Configure**.
2. Select an IP camera under **Camera Name**.
3. Under the **Rec Control** section, click the button after **Frames/Sec**. This dialog box appears.

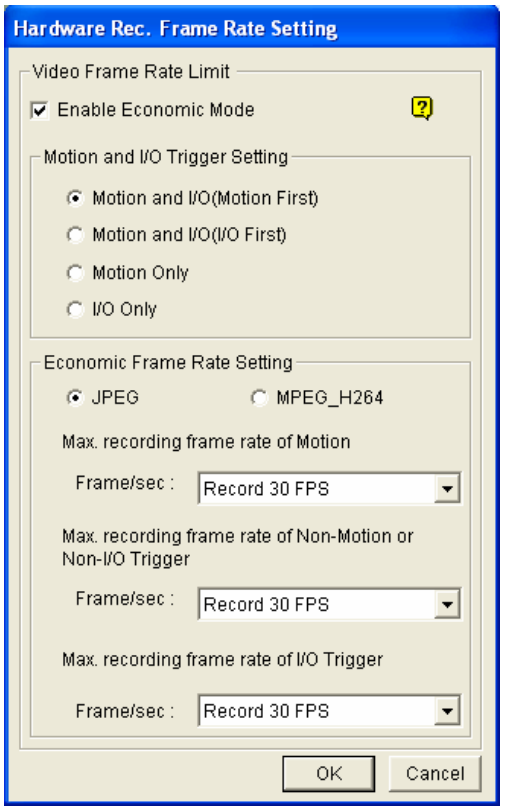


Figure 2-17

4. Select **Enable Economic Mode** to enable the economic mode.

5. Under the **Economic Frame Rate Setting** section, configure the frame rate settings for the incoming IP video compressed with **JPEG**, **MPEG** or **H264** codec.

   ⌘ To configure the frame rate setting for the IP video compressed with **JPEG**:

      A. Select **JPEG**.

      B. Specify the number of frame rates per second for different situations: when motion is detected (the **Max. Recording Frame Rate of Motion** option), when I/O devices are triggered (the **Max. Recording Frame Rate of I/O Trigger** option), when no motion is detected or when no I/O devices are triggered (the **Max. Recording Frame Rate of Non-Motion or Non-I/O Trigger** option).

   ⌘ To configure the frame rate setting for the IP video compressed with **MPEG** or **H.264**:

      A. Select **MPEG_H264**.

      B. Select to record in the maximum frame rate or record key frames only for different situations: when motion is detected (the **Max. Recording Frame Rate of Motion** option), when I/O devices are triggered (the **Max. Recording Frame Rate of I/O Trigger** option), when no motion is detected or when no I/O devices are triggered (the **Max. Recording Frame Rate of Non-Motion or Non-I/O Trigger** option).

6. Under the **Motion and I/O Trigger Setting** section, select one of the following options to specify the conditions to begin recording according to the Economic Frame Rate Setting you set in Step 5.

   ④ **Motion and I/O (Motion First):** The video images will be recorded according to your selection under the **Economic Frame Rate Setting** section when motion is detected or when the I/O device is triggered. However, when both motion detection and I/O trigger occur at the same time, the frame rate setting of motion detection will override the frame rate setting of I/O trigger.

   ④ **Motion and I/O (I/O First):** The video images will be recorded according to your selection under the **Economic Frame Rate Setting** section when motion is detected or when I/O devices are triggered. However, when both motion detection and I/O trigger occur at the same time, the frame rate setting of I/O trigger will override the frame rate setting of motion detection.

   ④ **Motion Only:** When motion is detected, the video images will be recorded according to your selection in **Max. Recording Frame Rate of Motion**.

   ④ **I/O Only:** When I/O devices are triggered, the video images will be recorded according to your selection in **Max. Recording Frame Rate of I/O Trigger**.

7. Click **OK** to apply the settings and select **Start All Monitoring** to run the application.

Note:

1. The **Max. Recording Frame Rate of Non-Motion or Non-I/O** option is only available when the camera is set to the **Round-the-Clock** recording mode.
2. The **Max. Recording Frame Rate** is subject to each camera's maximum frame rate.
3. When the video is recorded using JPEG compression method, every frame is a key frame.

2.11 On Demand Display

For cameras that support dual streaming with different resolutions, you can select the **On Demand Display** option to enable automatic adjustment of live view resolution. This option produces good image quality without causing high CPU usage.

You will need to set one video streaming of the camera to be higher than the other streaming. The system will switch to the higher resolution streaming when using view modes that require higher quality images, such as single view or PIP/PAP mode. When watching live view in view modes where higher resolution does not make a difference, such as a 16-channel screen division, the system will switch to the lower resolution streaming to reduce CPU usage.

To enable the function:

1. Make sure the IP camera has been added to the Main System and you have selected **Dual Stream** during setup. For details on how to add an IP camera, see *IP Channel Setup* earlier in this chapter.
2. Click the **Configure** button, select **System Configure**, select **Camera Install** and select **IP Camera Install**. The IP Device Setup dialog box appears.
3. Right-click the camera and select **On Demand Display**.

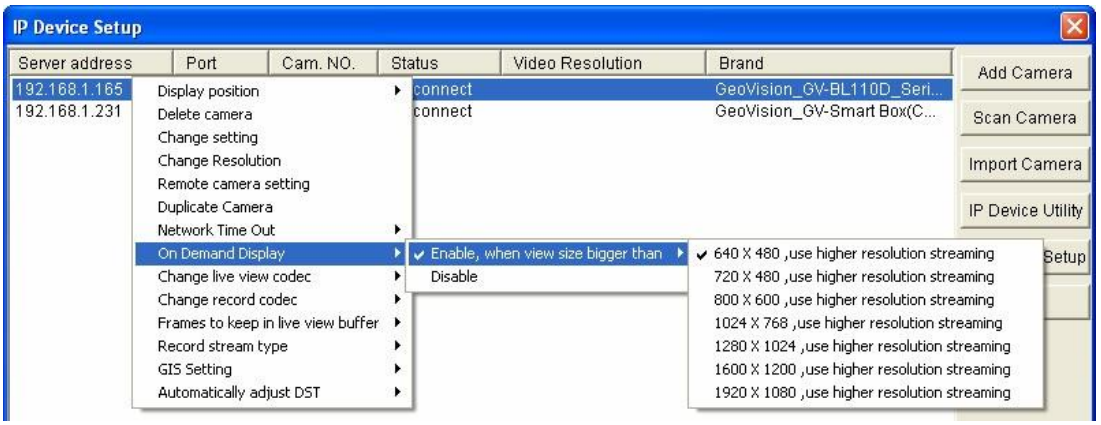


Figure 2-18

4. Point to **Enable, When View Size Bigger Than**, and select a resolution. When the resolution of the camera image on the screen is bigger than or equal to the selected resolution, the system will switch to the higher resolution streaming.

Note:

1. The **On Demand Display** function is not supported for **Privacy Mask**, **Defog** and **Stabilizer**.
2. The **On Demand Display** function is not supported for -Fisheye Camera.
3. If the same resolution has been set for both video streams, the On Demand Display option will still be visible, but automatic resolution adjustment will not occur.

Application Example

A resolution of 640 x 480 has been selected for the On Demand Display function.

- **Higher Resolution Streaming**

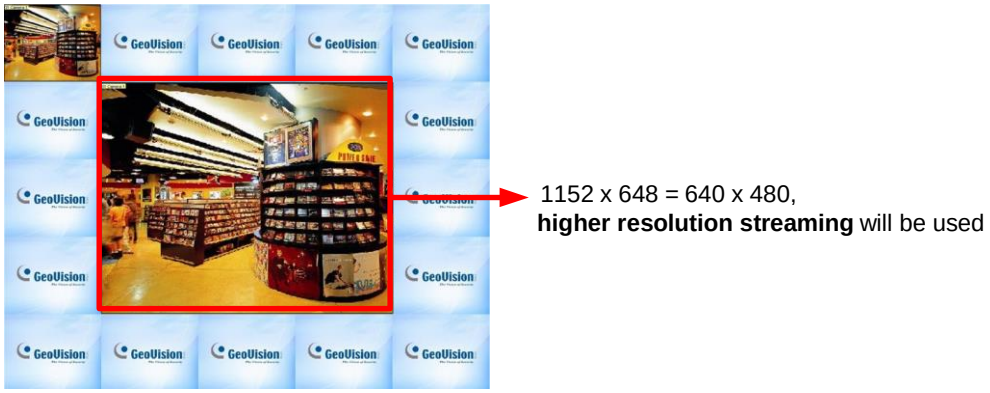


Figure 2-19

The camera image in the middle has a resolution of 1152 x 648, so the higher resolution streaming will be used, because 1152 x 648 is bigger than the selected 640 x 480.

- **Lower Resolution Streaming**

Figure 2-20

After switching to 16-channel screen division, the resolution for each channel is 480 x 270, which is smaller than the selected 640 x 480, so the lower resolution streaming will be used.

Chapter 3

Video Analysis 142

3.1 Object Tracking and Zooming 142

3.1.1 Object Tracking 142

3.1.2 Object Zooming 149

3.2 Advanced Single Camera Tracking 152

3.3 Digital Object Tracking 155

3.3.1 Setting Digital Object Tracking 155

3.3.2 Tracking in PIP View 157

3.3.3 Tracking in PAP View 158

3.4 Object Counting and Intrusion Alarm 159

3.4.1 Object Counting 160

3.4.2 Intrusion Alarm 164

3.5 Object Index 168

3.5.1 Setting Object Index 168

3.5.2 Viewing Object Index 170

3.5.3 Searching Object Index 171

3.6 Automatic Video Snapshots 173

3.6.1 Setting Video Snapshots 173

3.6.2 Searching Video Snapshots 175

3.7 Face Detection 177

3.8 Face Count 179

3.8.1 Installing the Camera 179

3.8.2 Setting Face Count 180

3.9 Unattended and Missing Object Detection 183

3.9.1 Detecting Unattended Objects 183

3.9.2 Detecting Missing Objects 185

3.10 Privacy Mask Protection 188

3.10.1 Setting a Privacy Mask 188

3.10.2 Granting Access Privileges to Recoverable Areas 189

3.11 Scene Change Detection 190

3.12 Panorama View 192

3.12.1 Stitching a Panorama View with Overlapping Areas 194
3.12.2 Easy Mode with No Overlapping Area 195
3.12.3 Accessing a Panorama View 198
3.13 Video Defogging 199
3.14 Video Stabilization 201
3.15 Wide Angle Lens Dewarping 203
3.16 Advanced Motion Detection 205
3.17 Crowd Detection 202
3.18 Advanced Scene Change Detection 210
3.19 Advanced Unattended Object Detection 213
3.20 Advanced Missing Object Detection 216
3.21 Video Analysis Schedule 219
3.21.1 Privacy Mask Schedule 221
3.22 Fisheye View 222
3.22.1 Setting Up a -Fisheye Camera 223
3.22.2 Setting Up a Third-Party Fisheye Camera 225
3.22.3 Object Tracking 225
3.23 Specifications 229

CHAPTER 3

Video Analysis

3.1 Object Tracking and Zooming

Object Tracking provides you the real-time tracking and automatic magnification of a single moving object by the combination of one PTZ camera and one stationary camera. If only one PTZ camera is available, it can be applied for Object Zooming, letting you configure four critical views for real-time zooming. The Object Tracking and Object Zooming functions can be combined together by completing both settings.

3.1.1 Object Tracking

For the tracking function, you need one PTZ camera applied for tracking and one stationary camera set for a fixed view. Install the PTZ camera and the stationary camera in close proximity of each other so the focus and the camera view of both are similar. Only -IP Speed Dome and some third-party IP cameras support this function. To see the supported PTZ cameras, see *Certified PTZ Models for Object Tracking* in *Appendix C*.

Setting Up a PTZ Camera

Before configuring the Object Tracking function, first configure the PTZ camera.

1. Click the **Configure** button (No. 14, Figure 1-2), select **Accessories**, select **PTZ Device** and select **PTZ Setup**.
2. Select the model from the drop-down list.
3. Click the button. A setup dialog box appears.

   - For -IP Speed Dome, select **Enable Object Tracking**. To configure the preset points, first select **Normal** and configure presets from the PTZ control panel on the screen.

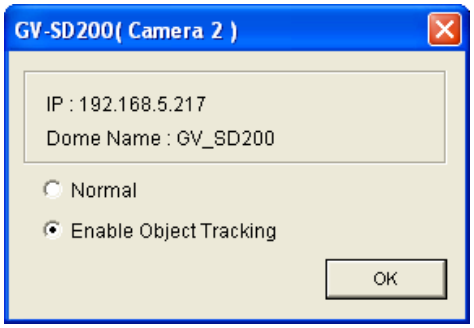


Figure 3-1

- For other cameras, select **Active** and select **Enable Object Tracking**. Specify **COM port**, **Baud Rate** and **PT Speed** of the PTZ camera. To configure the preset points, first select **Normal** and configure presets from the PTZ control panel on the screen.

4. Click **OK** to apply the settings.

Note: For analog cameras, you must first add the camera to the PTZ camera list. Click **Configure** button (No. 14, Figure 1-2), select **Accessories**, select **PTZ Device** and select **Add / Remove PTZ**. In the dialog box that appears, select the brand of your cameras and click the ›› button.

Setting up Object Tracking

After the above PTZ setup, go back to the main screen. Click the **Configure** button (No. 14, Figure 1-2), point to **Video Analysis**, select **Object Tracking Application**, and click **Object Tracking Setup** to display the following dialog box. The left image is the PTZ camera view and the right image is the stationary camera view.

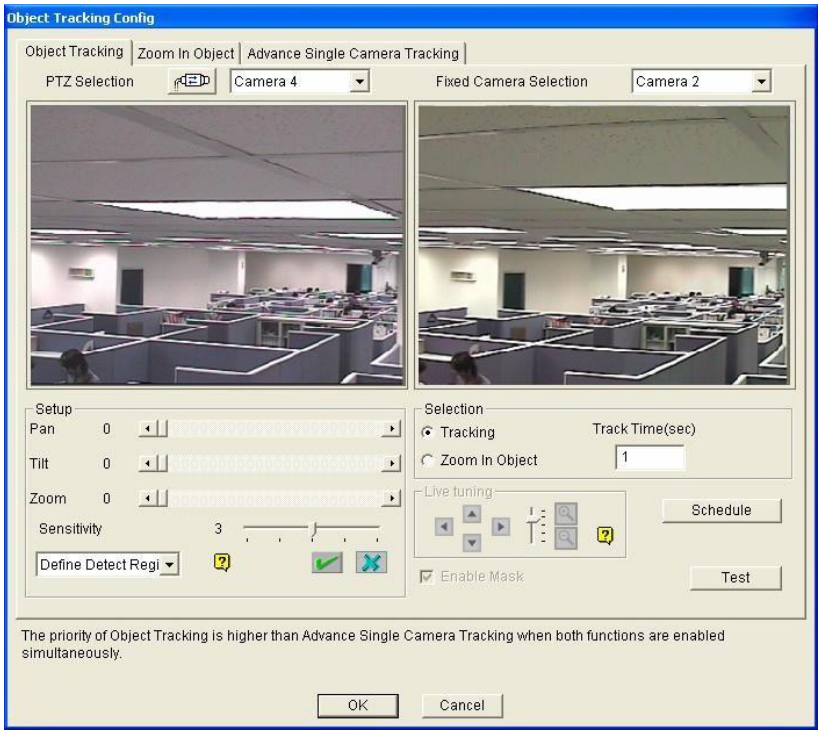


Figure 3-2

[PTZ Selection]

④ **:** Click to set up the PTZ.

④ **Camera:** Click the drop-down menu to choose the corresponding camera screen of the PTZ.

[Fixed Camera Selection] Click the drop-down menu to choose the corresponding camera screen of the stationary camera.

[Setup]

④ **Pan, Tilt and Zoom:** Use the slide bars to adjust the PTZ camera view.

④ **Sensitivity:** Use the slide bar to adjust the detection sensitivity.

④ **The drop-down menu:** Click the drop-down menu to define detection region and object size.

[Selection]

④ **Tracking:** Click to specify the tracking time.

④ **Zoom in Object:** Click to specify the idle time.

[Live Tuning] Adjust directions and the desired level of zooming.

[Schedule] Click to set up a schedule to enable the function.

[Enable Mask] Click to display the mask on the defined detection region when you test the settings.

1. Click to display the following dialog box, select the PTZ brand and the hardware address, and click **OK** to apply the settings.

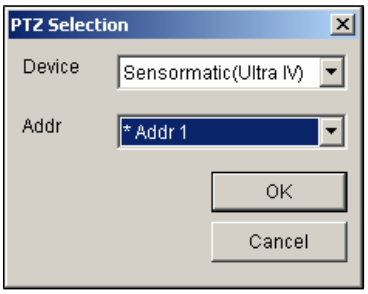


Figure 3-3

2. Choose the corresponding camera views of the PTZ and stationary cameras. In Figure 3-2, the images of the PTZ camera show in the Camera 2 view, while the images of the stationary camera show in the Camera 1 view.
3. Adjust the view of the PTZ camera with the sliders of Pan, Tilt and Zoom. Make sure the PTZ camera view is as similar as possible to the stationary camera view.
4. Click the **Save** button to save the both views as image references.
5. Adjust **Sensitivity** or keep it as default.

6. Select **Define Detect Region** from the drop-down menu. Use the mouse to outline a detection region in the right image; you will be prompted to enter **Detect Region**.

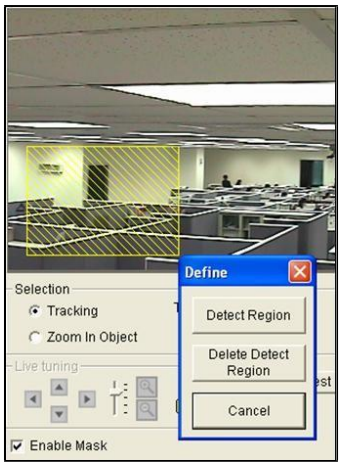


Figure 3-4

7. Select **Define Object Size** from the drop-down menu. Use the mouse to outline the max and min object sizes for tracking separately. Every time when finishing the outlining, you will be prompted to enter **Maximum Object Size** or **Minimum Object Size**.

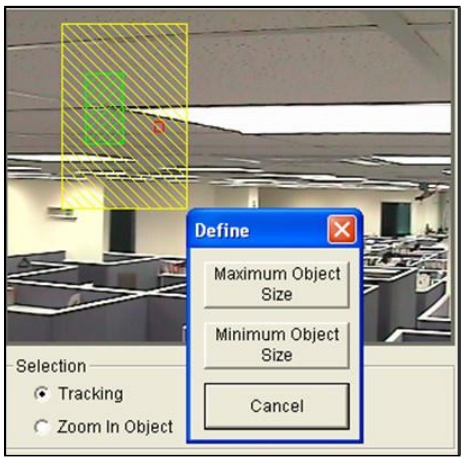


Figure 3-5

8. Click the **Tracking** item and specify **Track Time (sec)**. Track Time (sec) indicates the tracking duration in seconds.

Figure 3-6

9. When the PTZ is tracking, you can still control it to zoom in a desired area. Click the **Zoom in Object** item and specify **Idle Time (sec)**. Idle Time (sec) indicates the zooming duration in seconds. If a target appears after the specified idle time, the PTZ will start tracking. If not, the PTZ will remain on the zoomed place.

Figure 3-7

10. Click the **Schedule** button to set a schedule to enable the function. For details, see *Video Analysis Schedule* later in this chapter.
11. Click the **Test** button to check your settings. There are two major settings you have to observe in the testing. 1) Tracking: Observe if the target showing in the defined detection region is being tracked with a highlighted mask, and magnified automatically in the left image. If not, increase the sensitivity degree. 2) Zooming: Use the mouse to outline an object in the right image, and observe if it is magnified in the left image clearly. If not, use the **Live Tuning** buttons to adjust directions and the desired level of zooming.
12. Click **OK** to save your settings of the tracking time, the idle time for zooming in objects and the testing results.

Starting Object Tracking

After the above settings, you can start the object tracking application. Click the **Configure** button (No. 14, Figure 1-2), point to **Video Analysis**, select **Object Tracking Application**, and then click **Object Tracking Start** to start the function.

Tip: You can interrupt the PTZ camera tracking and take over the camera control by using PTZ Control Panel on Main System, PC's keyboard and accessories such as -Keyboard, -IR Remote Control, and -Joystick. When the controlling device or panel is inactive for over 5 seconds, the PTZ camera will go back for tracking.

Zooming in Objects

While the PTZ is being applied for tracking, you can still control it to zoom in any desired area by launching the Zoom in Dialog window.

1. Click the **Configure** button (No. 14, Figure 1-2), point to **Video Analysis**, select **Object Tracking Application**, and then click **Object Tracking View** to launch the Zoom in Dialog window, overlapping in the main screen, as shown below.

Note: The Zoom In Dialog window is for the stationary camera view and the main screen is for the PTZ view.

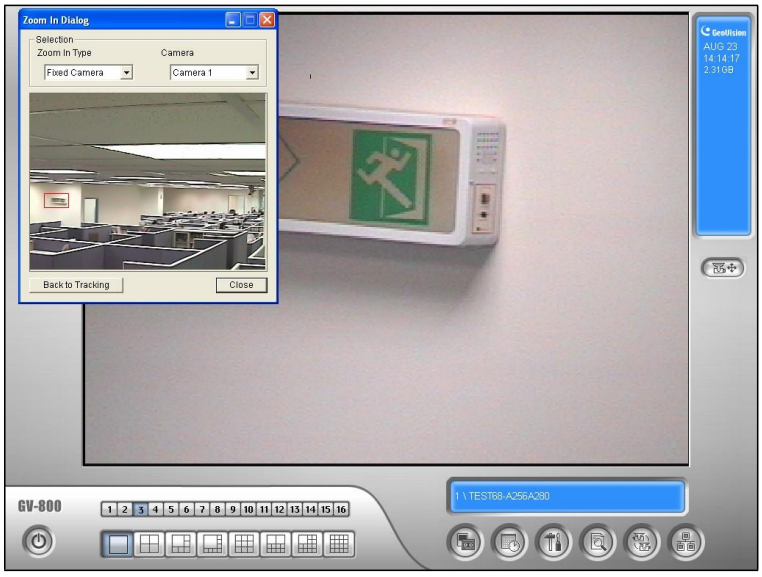


Figure 3-8 *The outlined area in the Dialog window is magnified on the main screen*

2. In the Zoom In Type field, select **Fixed Camera**.
3. In the Camera field, select the assigned camera view for the stationary camera.
4. Use the mouse to outline a desired area in the Dialog window. It will be magnified on the main screen.

When the specified idle time of zooming is up, PTZ will go back for tracking. If you want to stop the zooming function before the specified idle time, click the **Back to Tracking** button in the bottom of the Zoom In Dialog window. Then PTZ will go back to tracking instantly.

3.1.2 Object Zooming

If only one PTZ camera is available, without the stationary camera, you can simply apply it for the object zooming function. The feature allows you to configure up to 4 critical views for instant monitoring and zooming.

Setting up a PTZ Camera

Before configuring the Object Zooming function, first configure the PTZ device. Refer to *Setting up a PTZ Camera* in *Object Tracking* earlier in this chapter.

Setting up Object Zooming

After the above PTZ setup, go back to the menu bar.

1. Click the **Configure** button (No. 14, Figure 1-2), point to **Video Analysis**, select **Object Tracking Application**, and select **Object Tracking Setup** to display the Object Tracking Config dialog box. Then click the **Zoom in Object** tab in the upper part to display the following dialog box.

Note: The image on the right will not display until you complete the settings below.

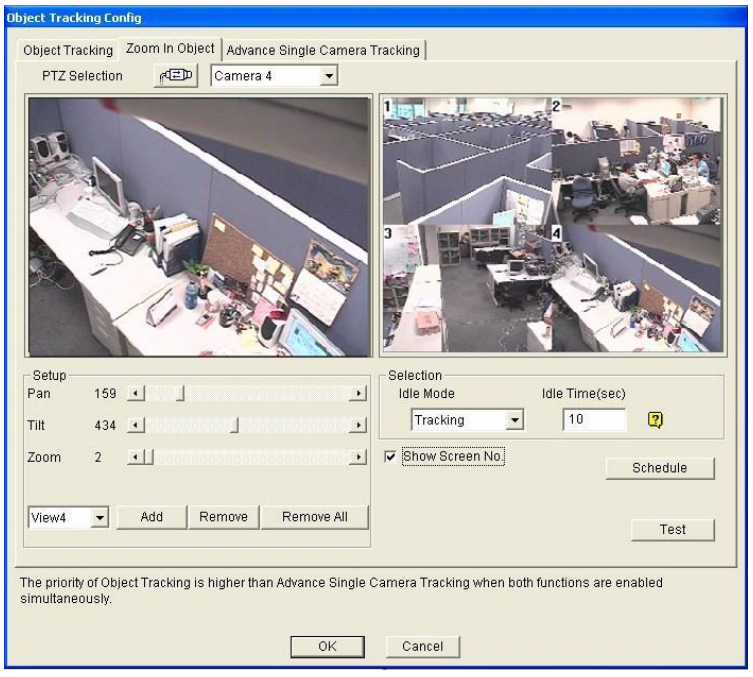


Figure 3-9

2. Click for the PTZ setup. Refer to *Object Tracking* earlier in this chapter.
3. Choose the camera view of the PTZ. In Figure 3-9, the images of the PTZ camera show in the camera 2 view.
4. Use the sliders of Pan, Tilt and Zoom to set up the View 1 as shown below. Then click the **Add** button to apply the settings. The View 1 will show in the upper-left corner of the right image.

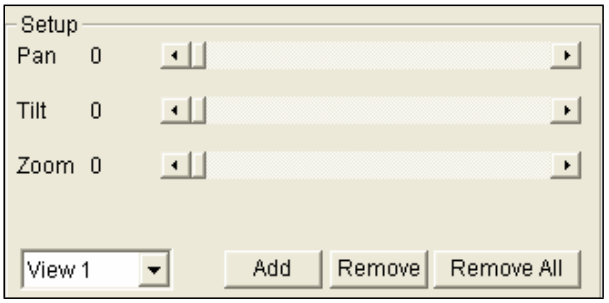


Figure 3-10

5. Click the drop-down menu to set up View 2, 3, and 4, one at a time. Refer to Step 4.
6. Specify **Idle Time (sec)**, indicating the zooming duration in seconds.

Figure 3-11

7. Click the **Idle Mode** drop-down menu. The seven options included inside are: **None**, **View 1**, **View 2**, **View 3**, **View 4**, **Tracking** and **Refresh View**.
   - ④ **None:** After zooming, the PTZ camera will remain on the same view until the next zooming command.
   - ④ **Tracking:** After the idle time, the PTZ camera will start tracking if it is also being applied for the tracking function.
   - ④ **View 1, 2, 3, 4:** After the idle time, the PTZ camera will go back to the preset View 1, 2, 3, or 4.
   - ④ **Refresh View:** After the idle time, the 4 views will be refreshed.

8. Click **Schedule** to set a schedule to enable the function. For details, see *Video Analysis Schedule* later in this chapter.
9. Click **Test** to check your settings. Use the mouse to outline a desired area in one of the four views. The area will be magnified in the left view.
10. Click **OK** to apply the displayed selections and close the dialog box.

Starting Object Zooming

After the above settings, you can start the object zooming application.

1. Click the **Configure** button (No. 14, Figure 1-2), point to **Video Analysis**, select **Object Tracking Application**, and click **Object Tracking View** to open the Zoom in Dialog window, overlapping on the main screen (Figure 3-8).
2. In the Zoom In Type field, select **Quad View**.
3. In the Camera field, select the assigned PTZ camera. Then the four views you set up before shows in the Zoom in Dialog window.

Figure 3-12

4. Use the mouse to outline a desired area in one of the four views. The area will be magnified on the main screen.
5. When you click the **Go to Idle Mode** button in the lower part, your setting in Step 7 of Object Zooming Setup will be applied. For example, if you choose View 3, the PTZ camera will go to the preset View 3 when you click the button.

3.2 Advanced Single Camera Tracking

The Advanced Single Camera Tracking can track a moving object using only one PTZ camera. When an object moves within the view of camera, the PTZ camera will follow its movement. When the object is out of view, the PTZ camera can be set to return to a designated position. For supported PTZ models, see *Certified PTZ Models for Object Tracking* in *Appendix C*.

Note: The Advanced Single Camera Tracking with color-based object tracking introduced in V8.3.2 has been removed. The Advanced Single Camera Tracking in V8.4 or later uses motion-based object tracking.

Setting up a PTZ Camera

Before setting up the Advanced Single Camera Tracking function, you need to first configure the PTZ device to enable Object Tracking. Refer to *Setting up a PTZ Camera* in *Object Tracking* earlier in this chapter.

Setting up Advanced Single Camera Tracking

1. Click the **Configure** button (No. 14, Figure 1-2), select **Video Analysis**, select **Object Tracking Application**, select **Object Tracking Setup** and click the **Advance Single Camera Tracking** tab. This dialog box appears.

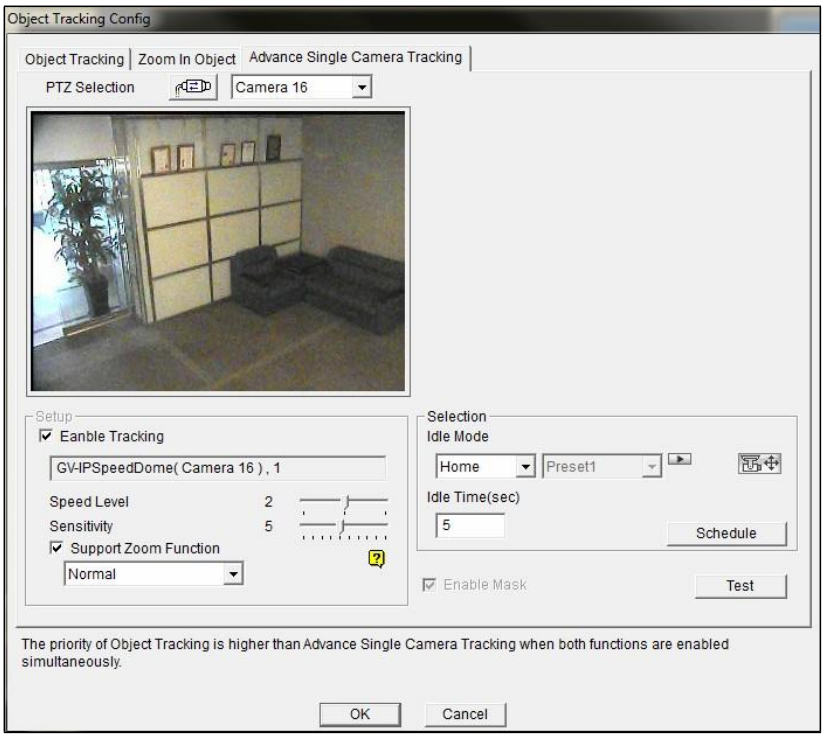


Figure 3-13

2. Select the camera from the **PTZ Selection** drop-down list.
3. Select **Enable Tracking**. This dialog box appears.

Figure 3-14

4. Specify the camera brand and its hardware address, and click **OK**.
5. Move the **Speed Level** slider to adjust the speed of PTZ movement. The higher the value, the faster the PTZ moving speed.

6. Select **Support Zoom Function** to be able to zoom in and out. Select **Normal** and the camera will zoom in once on the moving object. Select **Deep Zooming** and the camera will zoom in three times on the moving object.
7. Click the button to adjust the direction and zoom level of the camera.
8. To set the camera to return to its home position or a preset position when no motion is detected for a certain time period, specify **Idle Mode** and **Idle Time** in seconds. Click on the button to preview the designated position. Note that your camera will need to support home position and preset position.
9. To activate the function at certain times only, click the **Schedule** button and select **Active Schedule**. For details, see *Video Analysis Schedule* later in this chapter.
10. To outline a mask area where motion will be ignored, draw an area on the camera view and click **Set Mask** on the dialog box that pops up. To remove the mask, draw an area bigger than the mask, and click **Remove Mask**.
11. Click **Test**. Move an object through the view of camera and its movement should be tracked. If not, increase **Sensitivity** value to increase system sensitivity to motion in the camera view. If you have set a mask, you can select **Enable Mask** to display masked area during the test.
12. Click **OK** to apply the settings.
13. To begin single camera tracking, click the **Configure** button, select **Video Analysis**, select **Object Tracking Application**, and select **Object Tracking Start**.

Note: When multiple objects are moving at the same time, the camera will track the object with the largest area.

3.3 Digital Object Tracking

Without the need of a PTZ camera, the Digital Object Tracking provides you real-time tracking of up to 7 moving objects and automatic magnification of the targeted objects. The digital tracking function which combines with PIP View or PAP View can be an aid to spot any suspicious activities under the surveillance area.

3.3.1 Setting Digital Object Tracking

1. Click the **Configure** button (No. 14, Figure 1-2), click **Advanced Video Analysis**, and select **Digital Object Tracking Setting**.
2. Select the camera to be configured and click the **Configure** button. This dialog box appears.

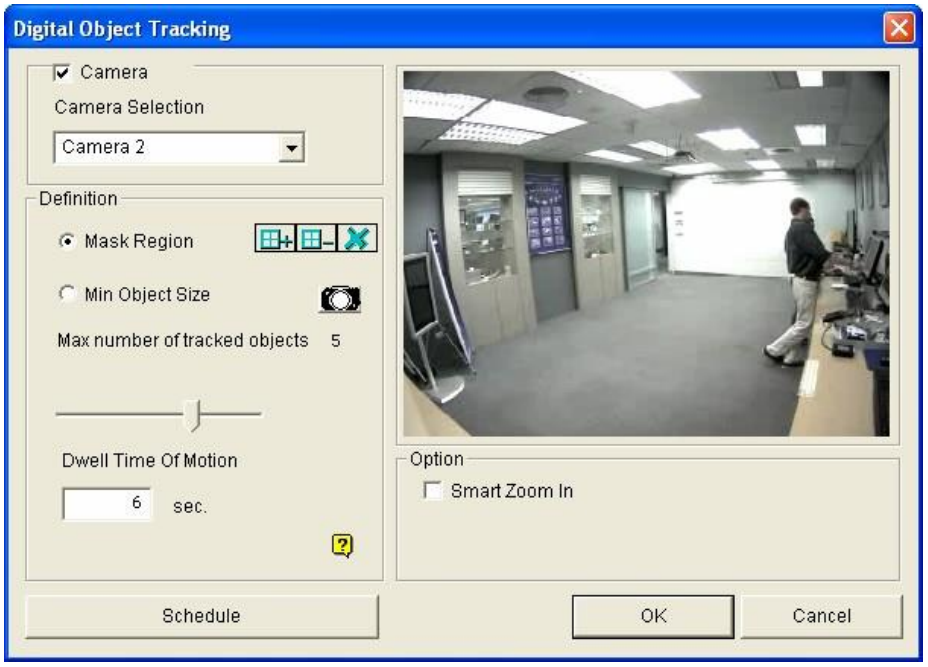


Figure 3-15

3. Select a camera from the Camera Selection drop-down list.

4. In the Definition section, there are three options:

   ④ **Mask Region:** Use the mouse to outline a mask area where motion will be ignored.

   ④ **Min Object Size:** First click the button to pause live images and then use the mouse to outline the minimum object size for tracking on the image.

   ④ **Max Number of Tracked Objects:** Use the slider to choose the maximum number of objects to be tracked. The maximum value is 7. This number also determines how many navigation boxes would be left free for selecting focus areas of interest in PAP View. See *Object Tracking in PAP View* later in this chapter.

   ④ **Dwell Time of Motion:** After a targeted object stops moving, the image will remain magnified for the number of seconds specified.

5. In the Option section, selecting **Smart Zoom In** can focus the upper part of the targeted object during tracking.

6. To activate the function at certain times only, click the **Schedule** button and select **Active Schedule**. For details, see *Video Analysis Schedule* later in this chapter.

7. Click **OK** to apply the settings.

Note:

1. The function will stop tracking an object when it remains stationary in the camera view for 3 seconds.
2. It takes about 3 to 5 seconds to start tracking after you switch to another channel for object tracking.

3.3.2 Tracking in PIP View

The PIP (Picture-in-Picture) View with Digital Object Tracking can track up to 7 moving objects and zoom in the first targeted object.

1. On the main screen, click the desired camera name label and select **PIP View**.
2. The screen automatically switches to one division, and an inset window of the camera view appears in the bottom right corner. Navigation boxes also appear inside the inset window to focus the moving objects.

Figure 3-16

3. The first object entering the camera view will be highlighted and zoomed in the live view screen. You can switch the highlight to another tracked object by clicking on its navigation box.

Note: Manually moving or adjusting the navigation box size is disabled in PIP View when Digital Object Tracking is enabled.

3.3.3 Tracking in PAP View

The PAP (Picture-and-Picture) View with Digital Object Tracking can create split video effects with up to 7 close-up views on moving objects.

1. On the main screen, click the desired camera name label and select **PAP View**.
2. The screen automatically switches to one division, and a row of inset windows appears around the live view screen. The number of inset windows is based on the number set for **Max Number of Tracked Objects**.

Figure 3-17

3. When a moving object enters the camera view, it will be highlighted with a navigation box to help you track the object. An inset window will also display the magnified image of the tracked object.
4. You could also draw the box to select a focus area, and this selected area is immediately reflected in one inset window. Up to (7 - **Max Number of Tracked Objects)** boxes can be drawn for focus areas. For instance, you can draw 5 boxes to be focus areas if you select 2 for the Max Number of Tracked Objects. See *Setting Digital Object Tracking* earlier in this chapter.
   - To delete a focus area, right-click a drawn box, select **Focus Area of PAP Mode** and select **Delete**.
   - To add another focus area when less than seven boxes are drawn, right-click the image, select **Mega Pixel Setting**, and select **Enable Add-Focus-Area-Mode**. Then draw a box on the image.

3.4 Object Counting and Intrusion Alarm

The Object Counting provides bi-directional counting of objects under the surveillance area. When defined, it could count any objects, such as people, vehicles, animals, etc.

The counter and intrusion alarm can be established with or without an AVP dongle. With an AVP dongle, you can set up the counter and intrusion alarm using lines to mark the boundary of detection zones. Without an AVP dongle, boxes are used for outlining the detection zones.

Note: The counter function is not suggested to be applied in Fisheye cameras.

1. Click the **Configure** button (No.14, Figure 1-2), point to **Video Analysis**, and then select **Counter/Intrusion Alarm Setting**. This dialog box appears.

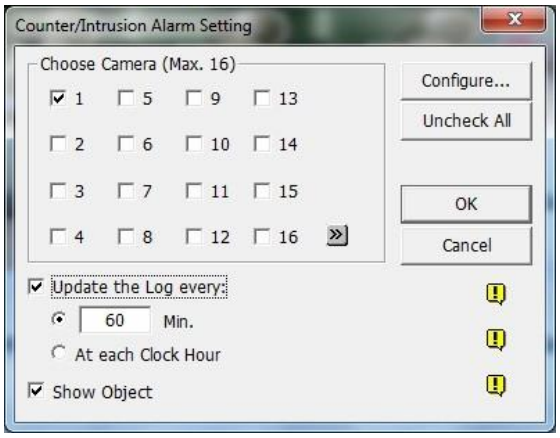


Figure 3-18

2. Select the desired cameras for the counter application.
3. Select **Update the Log** and specify the time interval in minutes to store the counting results to the System Log.
4. Select **Show Object** to put a rectangle around the object being tracked.
5. Click the **Configure** tab to open the Setup dialog box.

3.4.1 Object Counting

To define the counter to count target objects, click the **Counter** tab.

With an AVP Dongle

Set up the counter by using lines to mark the boundary of detection zones.

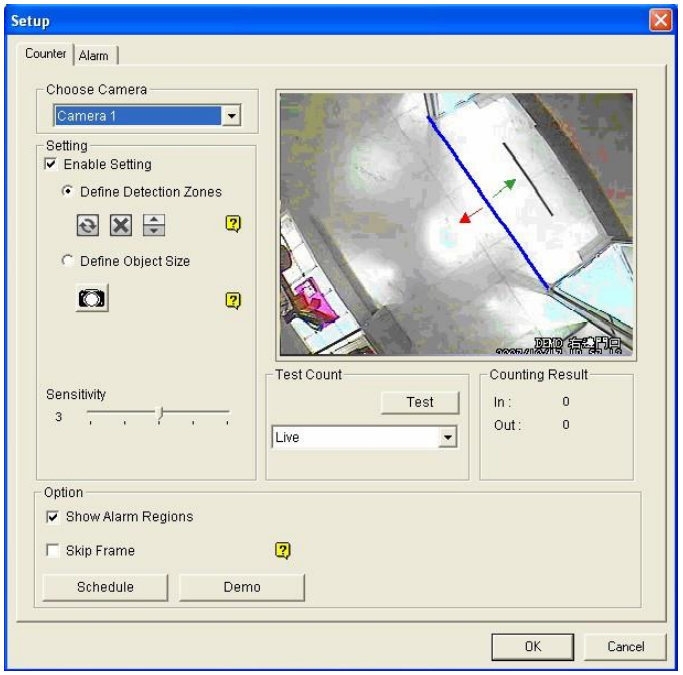


Figure 3-19

1. In the Choose Camera section, select a camera from the drop-down list for setup.
2. Select **Enable Setting** and set up the counter using the options below.

④ **Define Detection Zones:** Select this option and use the mouse to draw lines on the camera image to mark the boundaries of detection zones.

	This button is used to switch the direction and scheme of counting. Click this button to add green or red arrows or both. The **red arrow** indicates an in direction. When an object appears in the camera view and moves along the direction of the red arrow, it will be counted as 1 in. The **green arrow** indicates an out direction. When an object appears in the camera view and moves along the direction of the green arrow, it will be counted as 1 out.
	Click this button to switch to another detection zone and then use button to delete or the button to edit.
	Click this button to delete the detection zone.

④ **Define Object Size:** Select this option and click the button to pause live images. Use the mouse to outline a region matching the normal size of the targeted object.

3. To test your counting settings, select **Live** from the Test Count drop-down list and click the **Test** button to start testing. Notice how the number changes in the Counting Result section when objects move through the detection zone. Use the **Sensitivity** slider to increase or decrease detection sensitivity if the passing objects are not counted correctly.
4. To activate the function at certain times only, click the **Schedule** button and select **Active Schedule**. For details, see *Video Analysis Schedule* later in this chapter.
5. Click **OK** to apply the settings.
6. Start monitoring to begin counting.

More options in the Counter dialog box:

④ **Show Alarm Regions:** Displays the detection zones on the preview image.

④ **Skip Frame:** Skips frames when counting objects to lower the CPU loading. The system will count objects in every other three frames approximately. Note this option may reduce the accuracy of counting result.

④ **Embed Counting Results into Recorded Video:** Includes counting result in the recorded file.

Without an AVP Dongle

Set up the counter by drawing boxes to mark the detection zones.

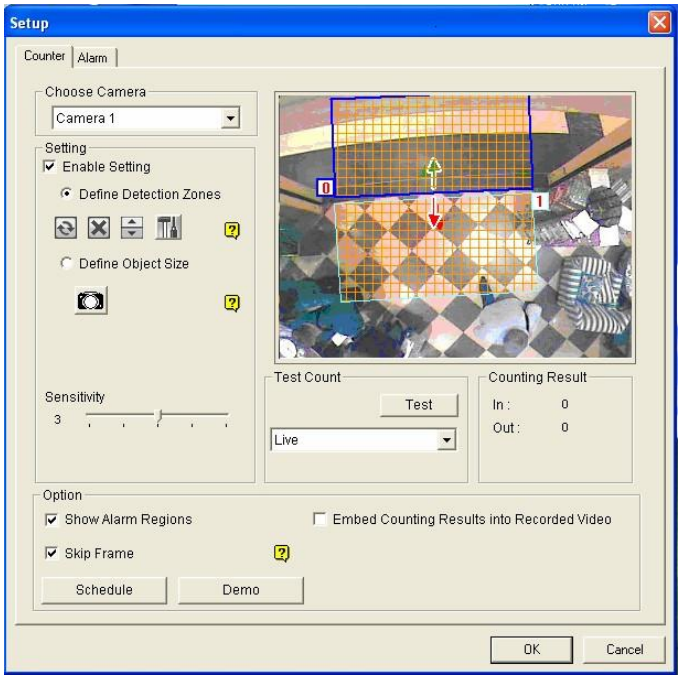


Figure 3-20

1. In the Choose Camera section, select a camera from the drop-down list for setup.
2. Select **Enable Setting** and set up the counter using the options below.

   ④ **Define Detection Zones:** Select this option to define the counter.

   a. On the live view, draw at least two boxes to mark the in and out detection zones. Each detection zone is numbered. You can use and to reverse or delete the detection zone. To switch to another detection zone, click the button.

   b. Click the button to define the in and out criteria. This dialog box appears.

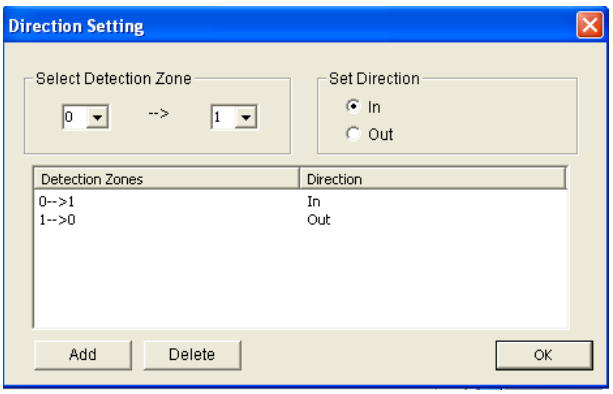


Figure 3-21

c. In the Set Direction section, select **In** and define the direction using the drop-down lists in the Select Detection Zone section.
d. Click the **Add** button. This setting appears under Detection Zones and Direction table.
e. Select **Out** in the Set Direction section, define the direction using the drop-down lists in the Select Detection Zone section, and click the **Add** button.
f. Click OK. The directions are indicated by arrows on the live view.

You have now set up the object counter with the in and out criteria defined. In the illustrated example (*Figure 3-20*), a target object is counted as in when it moves along the direction of the **red arrow** through detection zone 0 and 1, and the object is counted as out when it moves along the direction of the **green arrow** through detection zone 1 and 0.

④ **Define Object Size:** Select this option and click the button to pause live images. Use the mouse to outline a region matching the normal size of the targeted object.

3. To complete the counting setting, follow Steps 3 to 6 in *With an AVP Dongle* above.

Note: Draw the detection zones as closely as possible to avoid omission of counting when target objects show up from the unmarked area and move only through one of the two boundaries.

3.4.2 Intrusion Alarm

When any object crosses or is inside the defined region, the alarm can be activated for warning. To set the intrusion alarm, click the **Alarm** tab.

With an AVP Dongle

Set up the intrusion alarm by using lines to mark the boundary of detection zones.

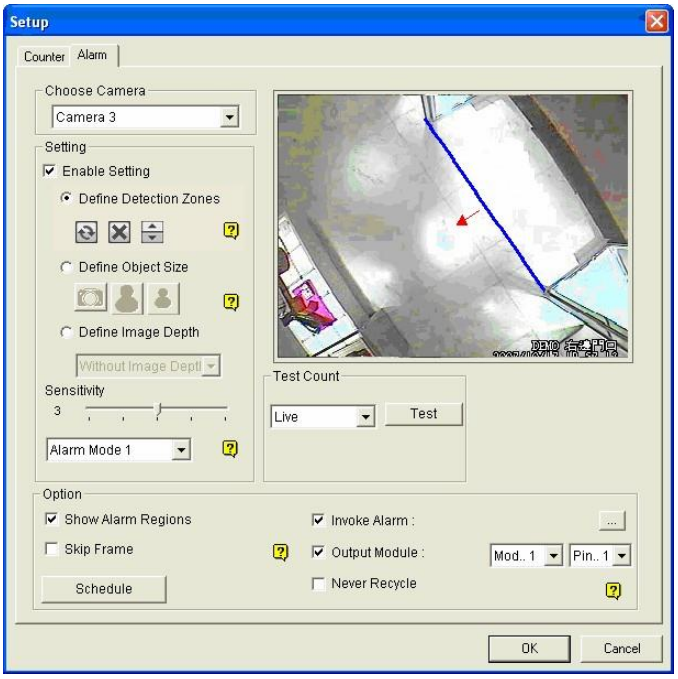


Figure 3-22

1. In the Choose Camera section, select a camera from the drop-down list for setup.
2. Select **Enable Setting** and define the targeted objects using the options below.
   - ④ **Define Detection Zones:** See Step 2 in *With an AVP Dongle* in *Object Counting* earlier in this chapter.
   - ④ **Define Object Size:** See Step 2 in *With an AVP Dongle* in *Object Counting* earlier in this chapter.

④ **Define Image Depth:** If the objects move toward or away from the camera along a path, a hallway for example, they will appear larger when getting closer to the camera and vice versa. You can select **With Image Depth** to define different object size according to the object's proximity to the camera. A line appears.

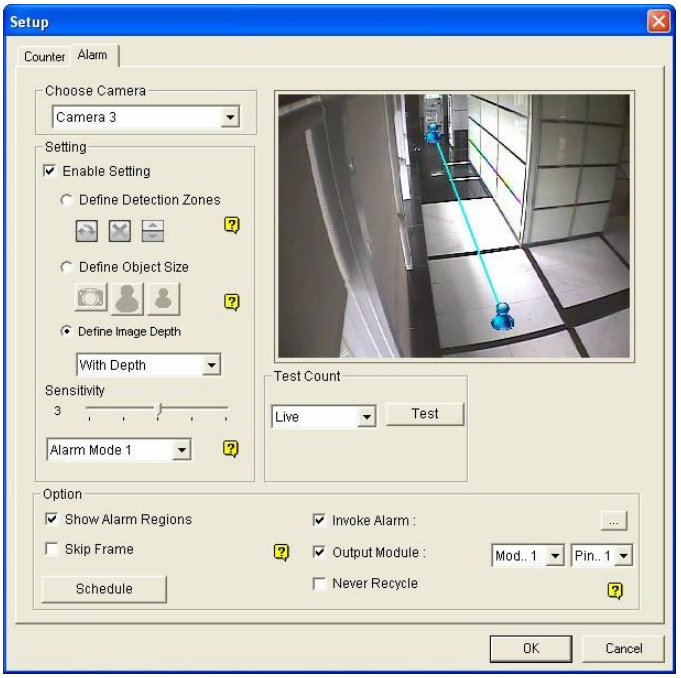


Figure 3-23

a. Place the line along the path where the objects will be moving by dragging the line. The larger icon indicates the point closer to the camera and the smaller icon indicates the point farther away from the camera.

b. Select **Define Object Size**. Click the larger icon and click the button to pause live images. Use the mouse to outline the maximum and minimum size of objects when they are close to the camera.

c. Click the smaller icon and repeat the step above to define the size of objects when they are far from the camera.

You have now defined two sets of object sizes at the two ends of the line.

3. In the Setting section, there are two kinds of alarm modes:

④ **Alarm Mode 1:** The alarm sets off when the target object moves through the first detection zone and touches the second detection zone in the defined direction.

④ **Alarm Mode 2:** The alarm sets off when the target object moves through the first detection zone and its center moves through the second detection zone in the defined direction.

4. To set up alarm devices, configure any or both of the following options.

④ **Invoke Alarm:** Enable the computer alarm when an object enters the defined region. Click the button next to the option to assign a .wav sound file.

④ **Output Module:** Enable an installed output device when an object enters the defined region. Assign the output module and pin number.

5. To test your alarm settings, select **Live** from the Test Count drop-down list and click the **Test** button to start testing. When the intrusion object is detected, the configured computer alarm or output device will be activated. Use the **Sensitivity** slider to increase or decrease detection sensitivity if the intrusion is not detected correctly.
6. To activate the function at certain times only, click the **Schedule** button and select **Active Schedule**. For details, see *Video Analysis Schedule* later in this chapter.
7. Click **OK** to apply the setting.
8. Enable monitoring to start intrusion detection.

When the intrusion event is detected, the configured computer alarm or output device will be activated, and the event will be recorded as **Intruder** in System Log for later retrieval.

More options in the Alarm dialog box:

④ **Show Alarm Regions:** Displays the detection zones on the preview image.

④ **Skip Frame:** Skips frames when detecting intrusion events to lower the CPU loading. The system will detect intrusion events in every other three frames approximately. Note this option may reduce the accuracy of detection.

④ **Never Recycle:** When the option is selected, the alarm-triggered events will not be recycled when recycle threshold is reached.

Without an AVP Dongle

Set up the intrusion alarm by drawing boxes to mark the detection zones.

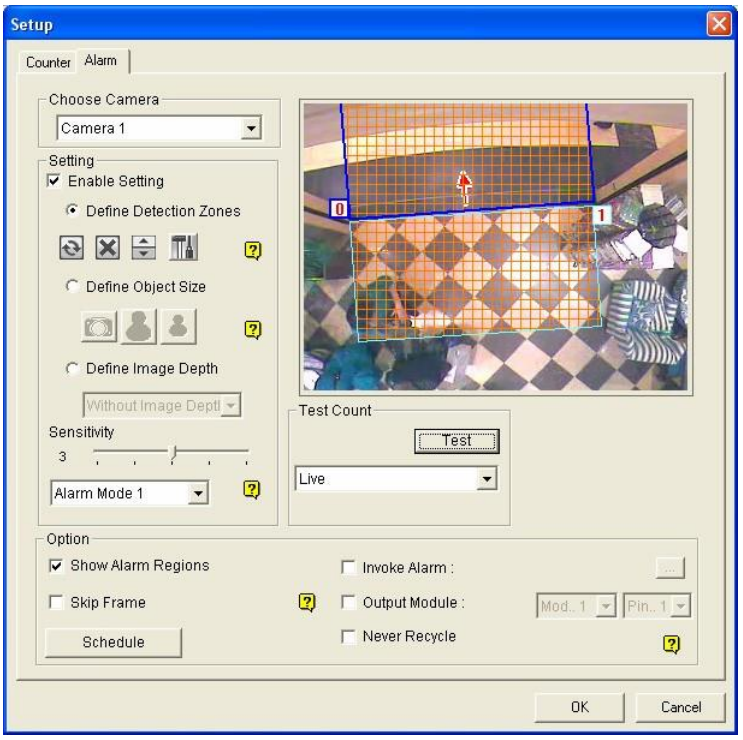


Figure 3-24

1. In the Choose Camera section, select a camera from the drop-down list for setup.
2. Select **Enable Setting** and define the targeted objects using the options below.
   ④ **Define Detection Zones:** Select this option to set up the counter.
   a. On the live view, draw at least two boxes to mark the in and out detection zones. Each detection zone is numbered. You can use and to reverse or delete the detection zone. To switch to another detection zone, click the button.
   b. Click the button to define the alarm criteria. This dialog box appears.

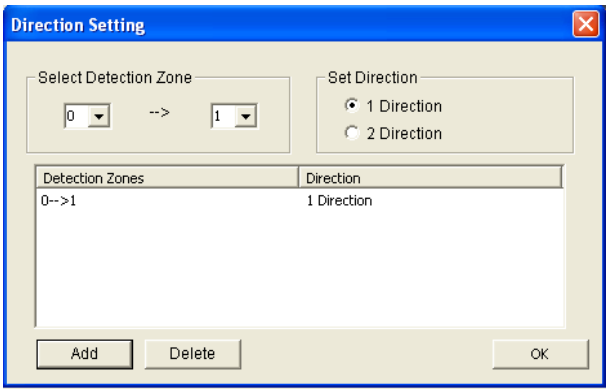


Figure 3-25

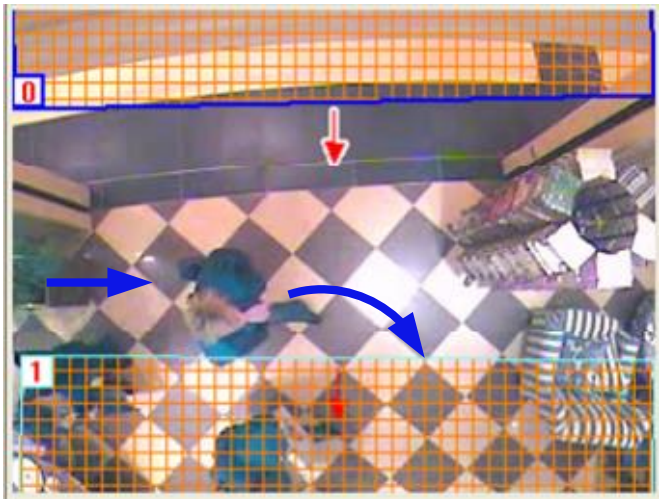
c. In the Set Direction section, select **1 Direction** for uni-direction or **2 Direction** for dual-direction criteria, and use the drop-down lists in Select Detection Zone section to define the direction.

d. Click the **Add** button. This setting appears in the Detection Zones and Direction table.

e. Click OK. The directions are indicated by arrows on the live view.

You have now set up the counter with the intrusion alarm criteria defined. In the illustrated example (*Figure 3-24*), when an object moves along the direction of the **red arrow** through detection zone 0 and 1, the alarm will be activated.

Note: Draw the detection zones as closely as possible to avoid omission of intrusion events when target objects show up from the unmarked area and only move through one of the two boundaries. In this case, the alarm will not set off.



---

④ **Define Object Size:** See Step 2 in *Without an AVP Dongle* in *Object Counting* earlier in this chapter.

3. To complete the intrusion alarm setting, follow Steps 3 to 8 in *With an AVP Dongle* in *Intrusion Alarm* earlier in this chapter.

3.5 Object Index

The Object Index feature allows you to view the very first frame of a *continuous* movement in a video stream. With Live Object Index, you may view the most recent 50 frames captured. With Object Index Search, you may easily locate a desired event and instantly play it back by double-clicking on the image frame.

3.5.1 Setting Object Index

You can select up to 16 cameras to view live video frames.

1. Click the **Configure** button (No. 14, Figure 1-2), point to **Video Analysis**, and then select **Object Index/Monitor Setup**. The Camera Applied Object Index/Monitor dialog box appears.
2. Select the desired cameras for the application.
3. Click the **Configure** button. The Video Object Setup window appears.

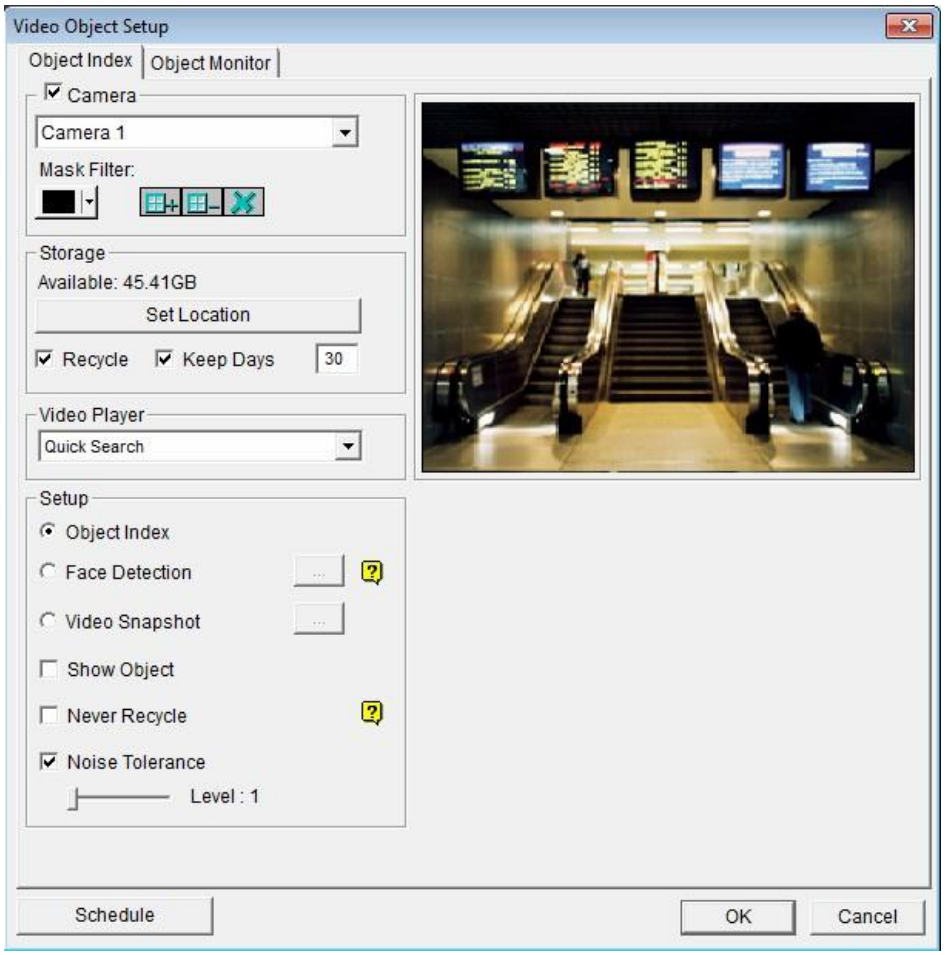


Figure 3-26 *Video Object Setup for Object Index*

4. Select one camera from the drop-down list and enable **Camera** for the following setup.
   - ④ **Mask Filter:** Use the mouse to outline a mask area where motion will be ignored.
   - ④ **Set Location:** Click the button to assign a path to save the file.
   - ④ **Keep Days:** Check the item and specify the days to store the files, from 1 day to 999 days.
   - ④ **Recycle:** When both Keep Days and Recycle are selected, the system applies whichever condition comes first. For example, if storage space is lower than that is required to hold the days of data specified in Keep Days, recycle comes first.
   - ④ **Video Player:** Select one of these players for playback function: ViewLog or Quick Search.
   - ④ **Show Object:** When motion is detected, it will be outlined with a blue frame.
   - ④ **Never Recycle:** With the option selected, the event files of object index and face detection will not be recycled when the recycle threshold is reached.
   - ④ **Noise Tolerance:** Use the slider to adjust the level. The higher the level, the more tolerant the system is to video noise.
5. In the Setup section, select **Object Index.**
6. Click **Schedule** to set a schedule to enable the function. For details, see *Video Analysis Schedule* later in this chapter.
7. Click **OK** to apply the settings.

Note: The minimum storage space required for Object Index is 500 MB.

3.5.2 Viewing Object Index

After configuring Object Index, you can start to view the most recent frames captured, with 50 frames at most.

1. Start camera monitoring.
2. Click the **ViewLog** button (No. 13, Figure 1-2), and then select **Live Object Index** to display the Live Viewer window.

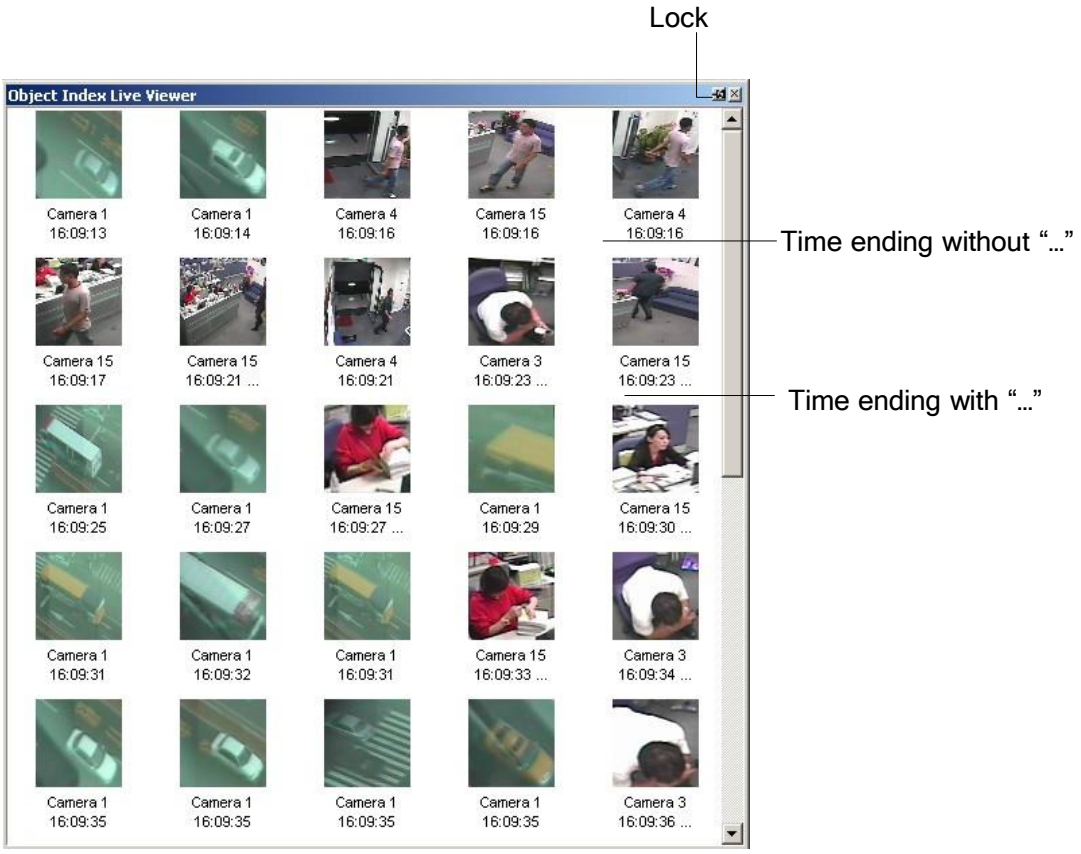


Figure 3-27

The controls in the Live Viewer window:

④ **The Lock button:** Click to pause the updating process.

④ **Time ending without "…":** This means the file is a complete one and can be played back with the ViewLog or Quick Search player. Double-click the frame to play back its related video.

④ **Time ending with "…":** This means the video can't be played back since the system is still recording.

3.5.3 Searching Object Index

You can locate frames within selected cameras and a specific time frame.

1. Click the **ViewLog** button (No. 13, Figure 1-2), and then select **Search Object Index** to display the following search window.

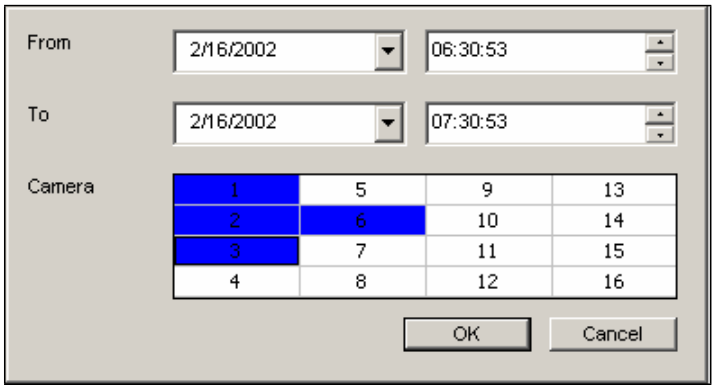


Figure 3-28 *The Search Window*

2. Specify a time frame and cameras, and then click **OK** to start searching. The following window will be called up.

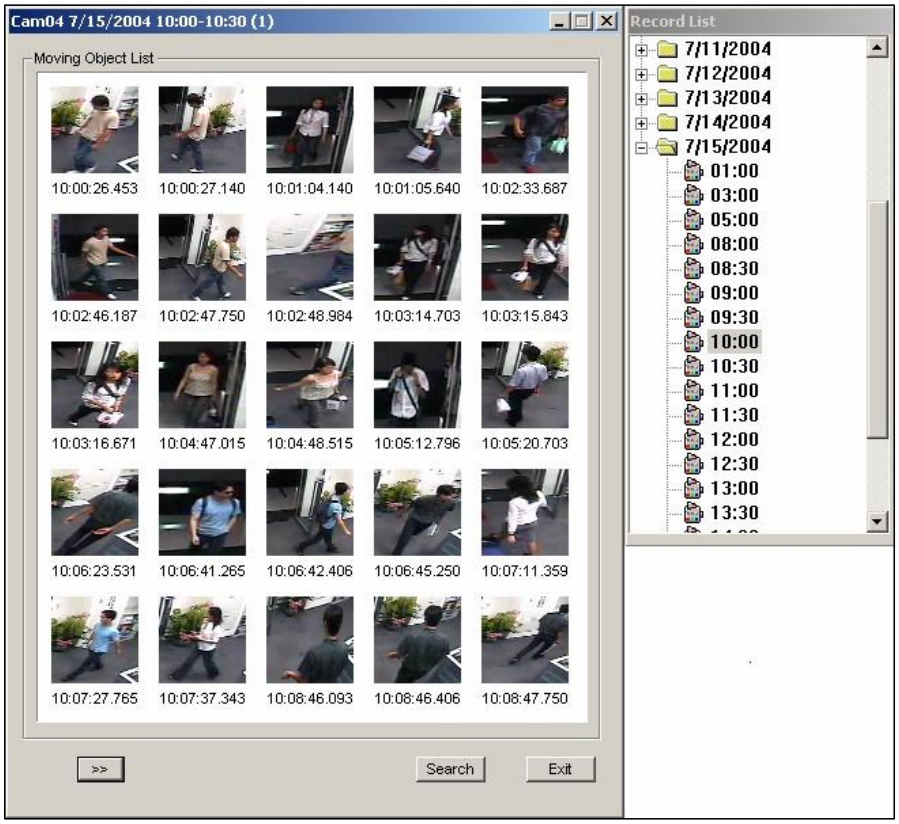


Figure 3-29 *The Moving Object List Window (left) and the Record List (right)*

[The Record List] The list contains the search results. Double-click a camera folder to display all found files. Click one time-segment file (e.g. 10:00) to open its included frames in the Moving Object List window.

[The Moving Object List window]

④ **Frames:** Double-click any frame in the window to play back its video file with the ViewLog or Quick Search player.

④ **:** Click the **Next Page** button for the next page.

④ **Search:** Click the button to launch the search window.

④ **Exit:** Click the button to close the window.

Note: Every time segment is a 30-minute interval, as shown in Record list in Figure 3-29.

3.6 Automatic Video Snapshots

The Video Snapshot allows the system to continuously take 2 snapshots every second as monitoring starts. This function gives you a choice to keep the surveillance images in still images or JPEG format when you don't have enough disk space to store AVI-format videos.

Note: After you start monitoring, the system will continue to take video snapshots whether there is motion or not.

3.6.1 Setting Video Snapshots

You can select up to 16 cameras to take video snapshots.

1. Click the **Configure** (No. 14, Figure 1-2) button, select **Video Analysis** and select **Object/Index Monitor Setup**. The Camera Applied Object Index/Monitor dialog box appears.
2. Select the desired cameras to be configured.
3. Click the **Configure** button. This dialog box appears.

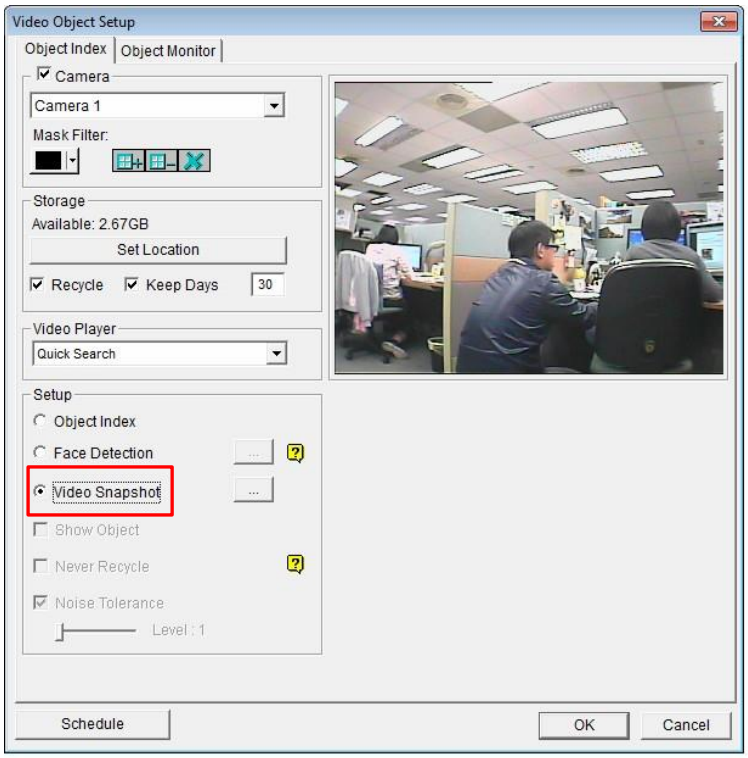


Figure 3-30

4. Select one camera from the drop-down list and enable **Camera**.

5. In the Setup section, select **Video snapshot**.
6. Click **[…]** after Video Snapshot for further setup.

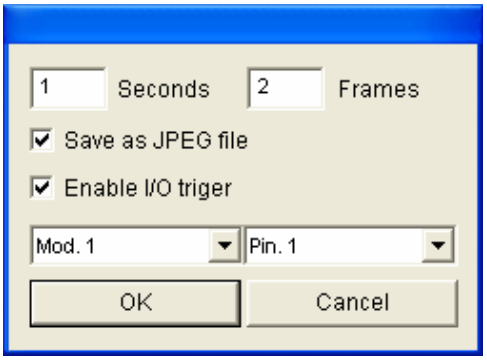


Figure 3-31

④ **Frames:** Specifies the frequency of automatic video snapshot. By default, the system will take 2 frames every second when the monitoring starts.

④ **Save as JPEG file:** Saves the images in JPEG format. Otherwise, you can only access the snapshots by using Quick Search and ViewLog players.

④ **Enable I/O Trigger:** Takes snapshots only when the assigned input device is triggered.

7. To activate the function at certain times only, click the **Schedule** button and select **Active Schedule**. For details, see *Video Analysis Schedule* later in this chapter.
8. Click **OK** to apply the settings
9. Start monitoring to take snapshots.

3.6.2 Searching Video Snapshots

You can locate snapshots within the specified cameras and period of time with **Object Index Search**.

1. Click the **ViewLog** button (No. 13, Figure 1-2), and select **Search Object Index**. This dialog box appears.

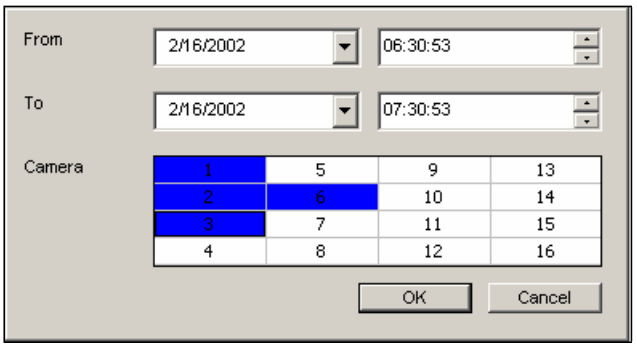


Figure 3-32

2. Specify a time period, select cameras, and click **OK** to start searching. The two windows appear.

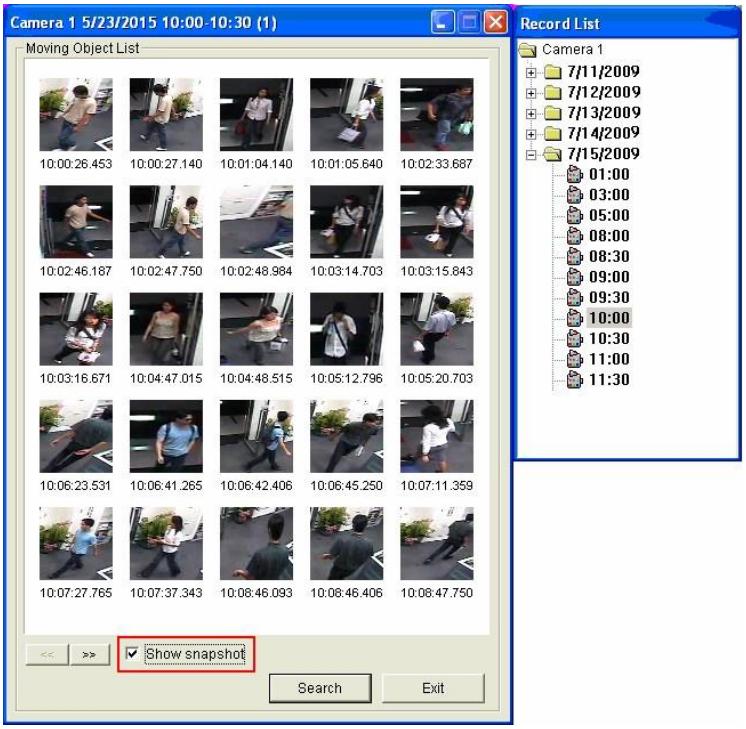


Figure 3-33

3. In the **Record List** window, expand a Camera folder to display all found date folders and time-segment files.
4. Click one time-segment file to open its included frames in the **Moving Object List** window.
5. To play images with Quick Search or ViewLog player, double-click the desired frame.
6. To display the image with your default image viewer of Windows, e.g. Paint, select **Show snapshot** at the bottom of the Moving Object List window and double-click the desired frame.

3.7 Face Detection

The Face Detection enables the -System to detect and record human faces. This feature captures human faces only, ignoring other body parts, objects or background views. Moreover, it can capture each face separately when a group of people comes in the view together.

Up to 16 cameras can be configured for this application.

1. Click the **Configure** button (No. 14, Figure 1-2), point to **Video Analysis**, and then select **Object Index/Monitor Setup**. The Camera Applied Object Index/Monitor dialog box appears.
2. Select the desired cameras to be configured.
3. Click the **Configure** button. The Video Object Setup window appears.
4. Select one camera from the drop-down list and select **Camera** to enable the following settings.
5. In the Setup section, select **Face Detection**.
6. Click **[…]** after Face Detection to adjust the sensitivity. The higher the value, the more sensitive face detection is.
7. Select **Noise Tolerance** and use the slider to adjust the level. The higher the level, the more tolerant the system is to video noise.
8. Click **OK**.
9. Start the monitoring of the configured camera(s).
10. On the main screen, click the **ViewLog** button (No. 13, Figure 1-2) and select **Live Object Index**. When the faces are detected, the thumbnail images will appear on the Object Index Live Viewer.

Figure 3-34

11. Double-clicking one of images can play back its related video.

For details on the settings in the Video Object Setup dialog box, see *Setting Object Index* earlier in this chapter.

Note:

1. Face contour must be clearly seen.
2. Only faces tilting within the range of 15° vertically and 30° ~ 45° horizontally can be detected.
3. The face to be detected must cover at least 1/10 of the screen.

3.8 Face Count

The Face Count function allows you to count the number of faces that appear in the image. You can also select to invoke a computer alarm or trigger an output device when a face is detected or when the system is unable to detect a face.

The number of faces counted is saved to the -Web Report, and the -Web Report can analyze counting data from multiple -Systems. For details, see *-Web Report User's Manual*.

Note: Up to 16 cameras can be configured for this function.

3.8.1 Installing the Camera

1. Install the camera inside an entrance pointing horizontally outward. The Face Count function is designed to detect front-view faces only, and the area of the detected face must take up 10% to 50% of the live image.

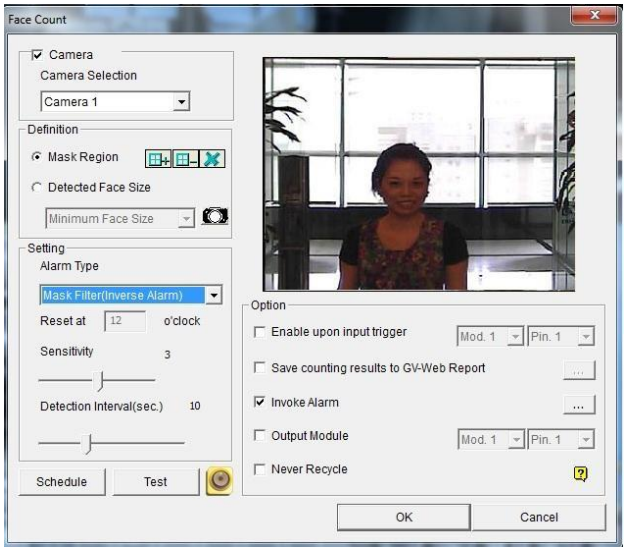


Figure 3-35

2. Avoid installing the camera where it can be subjected to direct sunlight or reflections. The lighting of the entrance where you set the camera should be sufficient but not be too bright or dark. Light should be distributed evenly across faces without too much light coming from one side. If sharp shadow edges are visible in the camera view, the count accuracy might be less than what it normally is.

3.8.2 Setting Face Count

1. Click the **Configure** button (No. 14, Figure 1-2), select **Advanced Video Analysis**, and click **Face Count Setting**.
2. Select the cameras you would like to configure, and click **Configure**. This dialog box appears.

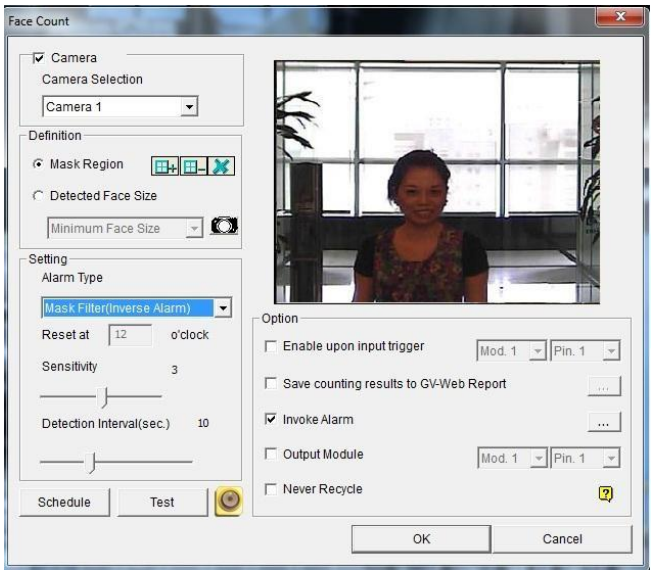


Figure 3-36

3. Under **Camera Selection**, select a camera from the drop-down list to be configured.
4. The following configurations are available:

[Definition]

④ **Mask Region:** Use the mouse to outline a mask area where motion will be ignored.

④ **Detected Face Size:** You can adjust the **Minimum Face Size** and the **Maximum Face Size** to instruct the system to only detect faces within that size range. You must pause the live image by clicking the button before you can adjust the size.

[Setting]

④ **Alarm Type**

⌘ **Face Count:** Counts the number of faces. The counting results are only available on the -Web Report. To connect to the -Web Report, refer to the **Enable Web Report** option below.

⌘ **Mask Filter:** Detects faces and invokes a computer alarm or triggers an output device.

⌘ **Mask Filter (Inverse Alarm):** Invokes a computer alarm or triggers an output device when the system is unable to detect a face after the number of seconds specified in the **Detection Interval**.

④ **Reset at:** Type a counting reset time between 0 and 23. For example, if you type 23, the number of faces counted will become zero at 23 o'clock daily.

④ **Sensitivity:** Adjust the detection sensitivity by moving the slider. The higher the value the more sensitive the system to motion. The default value is 3.

④ **Detection Interval:**

⌘ When **Mask Filter** and **Input I/O Trigger** are both selected, the **Detection Interval** slider specifies the number of seconds you want the system to detect faces when the input device is triggered. For example, the input device is a card reader and a door lock has been set up as the output device. After you swipe the card triggering the reader, the system starts to detect the face for the interval specified. If the face is detected within the interval, the door will be open; otherwise the door will remain locked.

⌘ When **Mask Filter (Inverse Alarm)** is selected, the system will attempt to detect the faces for the number of seconds specified. For example, if you set the interval to 15 seconds, the alarm will be triggered if the system cannot detect any faces within 15 seconds after motion is detected.

[Option]

④ **Enable upon input trigger:** The system will begin detecting only when the input device is triggered. Assign an input module and pin number for the device.

④ **Saves counting results to -Web Report:** Saves the face counting results to the -Web Report. When the option is selected, the dialog box below appears. Type the **Domain Name or IP Address**, **Port**, **UserName**, and **Password** of the -Web Report. After settings, click the **Test** button to see if the connection is succeeded.

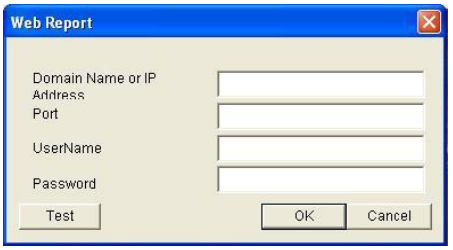


Figure 3-37

④ **Invoke Alarm:** Activates the computer sound alarm when faces are detected under **Mask Filter** or when the system is unable to detect faces under **Mask Filter (Inverse Alarm)**. Click the **[…]** button to designate a sound file to be the alarm sound.

④ **Output Module:** Activates the output device when faces are detected under **Mask Filter** or when the system is unable to detect faces under **Mask Filter (Inverse Alarm)**. Assign an output module and pin number for the device.

④ **Never Recycle:** Prevents recorded events from being recycled when the recycle threshold is reached.

5. Click the **Test** button to see if the settings have been configured according to your preference. If you have set a detection interval, the test will only run for the number of seconds you specified.
6. To activate the function at certain times only, click the **Schedule** button and select **Active Schedule**. For details, see *Video Analysis Schedule* later in this chapter.
7. Click **OK** to apply the settings.
8. Start monitoring to run the application.

Note:

1. Events triggered under **Mask Filter** or **Mask Filter (Inverse alarm)** will be recorded to the System Log, and can be played back in ViewLog. In the System Log, the events are recorded as **Face Count** under the **Event** column.
2. The face counting results will only be saved when **Enable Web Report** is selected and the -Web Report is connected.
3. The counter function is not suggested to be applied in fisheye cameras.

3.9 Unattended and Missing Object Detection

The Object Monitor program can detect any unattended and/or missing object within the camera view by highlighting its location.

3.9.1 Detecting Unattended Objects

To detect any unattended objects within the camera view, follow the steps below:

1. Click the **Configure** button (No. 14, Figure 1-2), select **Video Analysis**, and select **Object Index/Monitor Setup**. The Camera Applied Object Index/Monitor dialog box appears.
2. Select the desired cameras for the application.
3. Click the **Configure** button. The Video Object Setup dialog box (Figure 3-25) appears.
4. Click the **Object Monitor** tab. This dialog box appears.

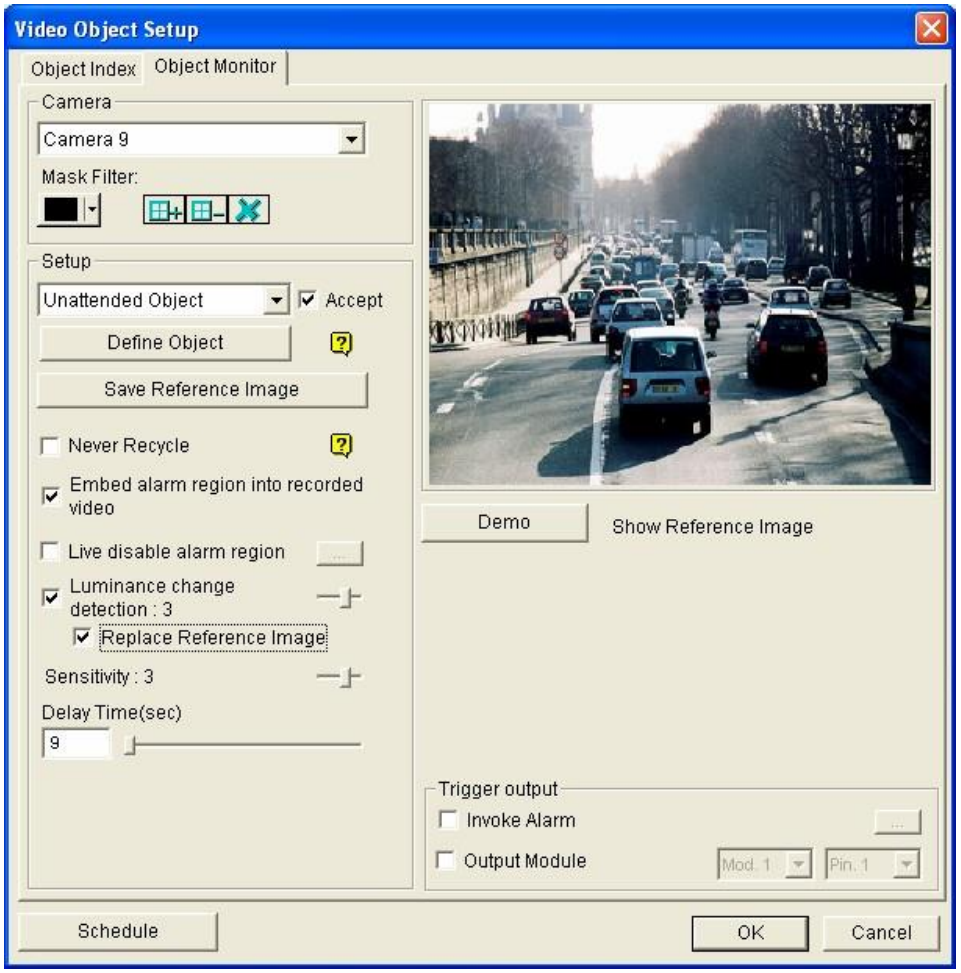


Figure 3-38 *Object Monitor*

5. In the Camera field, select a desired camera for setup.
6. Select **Unattended Object** from the drop-down list.
7. Click the **Accept** check box to make other options available.
8. Use the **Mask Filter** function to ignore any motion detection within a certain area if necessary.
9. Click the **Define Object** button.
10. Use the mouse to outline the max and min detection regions separately on the screen. Every time when finishing an outlining, you will be prompted to select **Maximum Size** or **Minimum Size**. See the illustration below.

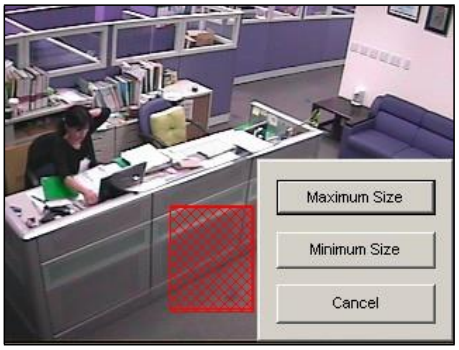


Figure 3-39 *Defining the min. and max. detection size*

11. Click the items of **Show Max** and **Show Min** in the lower of the window one by one to check your defined sizes.
12. Click the **Done** button to finish the defining.
13. Click the **Save Reference Image** button to save the image as a reference view.
14. To set up other options, see *Other controls in the Video Object Setup window* in the section of *Detecting Missing Object* later in this chapter.
15. To activate the function at certain times only, click the **Schedule** button and select **Active Schedule**. For details, see *Video Analysis Schedule* later in this chapter.
16. Click the **OK** button to apply the settings.
17. Start camera monitoring for the application.

When an unattended object appears and remains stationary for 9 seconds, its location will be highlighted in live video, the selected alarm and output will be activated, and the event will be recorded as **Unattended Object** in System Log for later retrieval.

3.9.2 Detecting Missing Objects

To detect any object missing from the camera view, follow the steps below:

1. Follow the Step 1 to 4 in the above *Detecting Unattended Objects* section to display the Video Object Setup dialog box (Figure 3-26).
2. In the Camera field, select a desired camera for configuration.
3. Select **Missing Object** from the drop-down list.
4. Check the **Accept** option to make other options available.
5. Click the **Define Object** button.
6. Use the mouse to outline regions on the object(s) you want to detect. It is recommended to outline several regions within the object(s) to increase detection sensitivity. Notice that the outlined regions should not be larger than the object(s). Every time when finishing an outlining, you will be prompted to select **Add Region**. See the illustration below.

Figure 3-40 *Outlining regions on objects*

7. Click the **Done** button to finish the defining.
8. Click the **Save Reference Image** button to save the image as a reference view.
9. To set up other options, see *Other Controls in the Video Object Setup Window* below.
10. Click the **OK** button to apply the settings.
11. Start camera monitoring for the application.

When any object, which you have outlined the regions for, disappears from the camera view for 3 seconds, its location will be highlighted in live video, the selected alarm and output will be activated, and the event will be recorded as **Missing Object** in System Log for later retrieval.

Other Controls in the Video Object Setup Window:

④ **Show Reference Image:** Click to view the saved reference image.

④ **Never Recycle:** When this option is selected, the events of unattended and missing objects will not be recycled when the recycle threshold is reached.

④ **Embed Alarm Region into Recorded Video:** This option will contain the flashing alert boxes in the recorded files so you can easily find out suspicious events during playback. Note that if you are used to searching suspicious events with Object Search, do not enable this option. These flashing boxes can cause false alarms.

Live Disable Alarm Region: When an unattended or a missing object is detected, this option allows you to close the flashing alert box automatically or manually. Under **Delay Time(s)**, specify the duration of an unattended or a missing object to invoke a warning message (Figure 3-41). The range of delay time is from 1 to 99999 seconds.

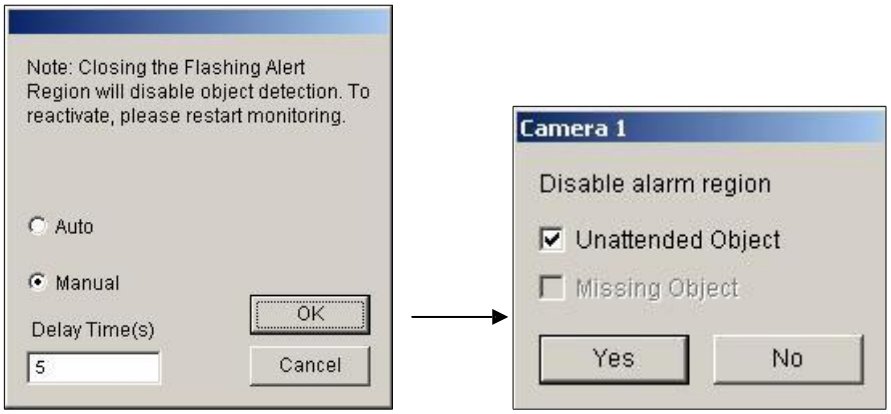


Figure 3-41 ***Figure 3-42***

④ **Luminance Change Detection:** This option may suspend object detection when the lighting condition is poor so as to avoid false detection. Use the slide bar to adjust the level of detection from 1 to 5. The higher the level is, the more sensitive the system is to luminance change. When luminance change reaches the level you set, the system will stop object detection.

④ **Sensitivity:** Use the slide bar to increase or decrease detection sensitivity if necessary.

④ **Delay Time:** This option allows you to specify the duration of an object missing or unattended to invoke the detection.

Unattended Object: The duration is from 3 to 1800 seconds, with 3 seconds as default.

For example, suppose you choose 12 seconds. When an unattended object appears in the camera view for 12 seconds, its location will be highlighted.

Missing Object: The duration is from 3 to 1800 seconds, with 3 seconds as default. For example, suppose you choose 9 seconds. When a defined object disappears from the camera view for 9 seconds, its location will be highlighted.

④ **Invoke Alarm:** Enables the computer alarm when any unattended and/or missing objects are detected. Click the **[…]** button next to the item to assign a .wav sound file.

④ **Output Module:** Activates the output device when any unattended and/or missing object is detected. Click the **[…]** button next to the item to assign an installed output module and a pin number.

④ **Demo:** Click to see the demonstration from actual DVR applications.

3.10 Privacy Mask Protection

The Privacy Mask can block out sensitive areas from view, covering the areas with black boxes in both live view and recorded clips. This feature is ideal for locations with displays, keyboard sequences (e.g. passwords), and for anywhere else you don't want sensitive information visible.

You can also choose to retrieve the block-out areas during playback. The retrievable areas will be protected by password.

3.10.1 Setting a Privacy Mask

1. Click the **Configure** button (No. 14, Figure 1-2), point to **Video Analysis**, and then select **Privacy Mask Setting**. The Privacy Mask Setup dialog box appears.
2. Select the desired cameras for setup, and then click the **Configure** tab. This dialog box appears.

Figure 3-43 *Privacy Mask Setup*

3. Select a camera from the drop-down list, and select **Enable**.
4. Select Un-recoverable and/or Recoverable.
   - ④ **Un-recoverable:** You cannot retrieve the block-out area(s) in the recorded clips.
   - ④ **Recoverable:** The block-out area(s) is retrievable with password protection.
5. Drag the area(s) where you want to block out on the image. You will be prompted to click **Add** to save the setting. The Un-recoverable region is marked in black, while the recoverable region is shown in red.
6. Click **Schedule** to set a schedule to enable the function. For details, see *Video Analysis Schedule* later in this chapter
7. Click **OK** to save the settings.

3.10.2 Granting Access Privileges to Recoverable Areas

The user must be granted access privileges to see the block-out areas when launching ViewLog for playback.

1. Click the **Configure** button (No. 14, Figure 1-2), point to **System Configure**, select **Password Setup**, and select **Local Account Edit**. The Password Setup dialog box appears.
2. Select one account, click the **Privacy Mask** tab, and check **Restore Recoverable Video** to grant the privilege.

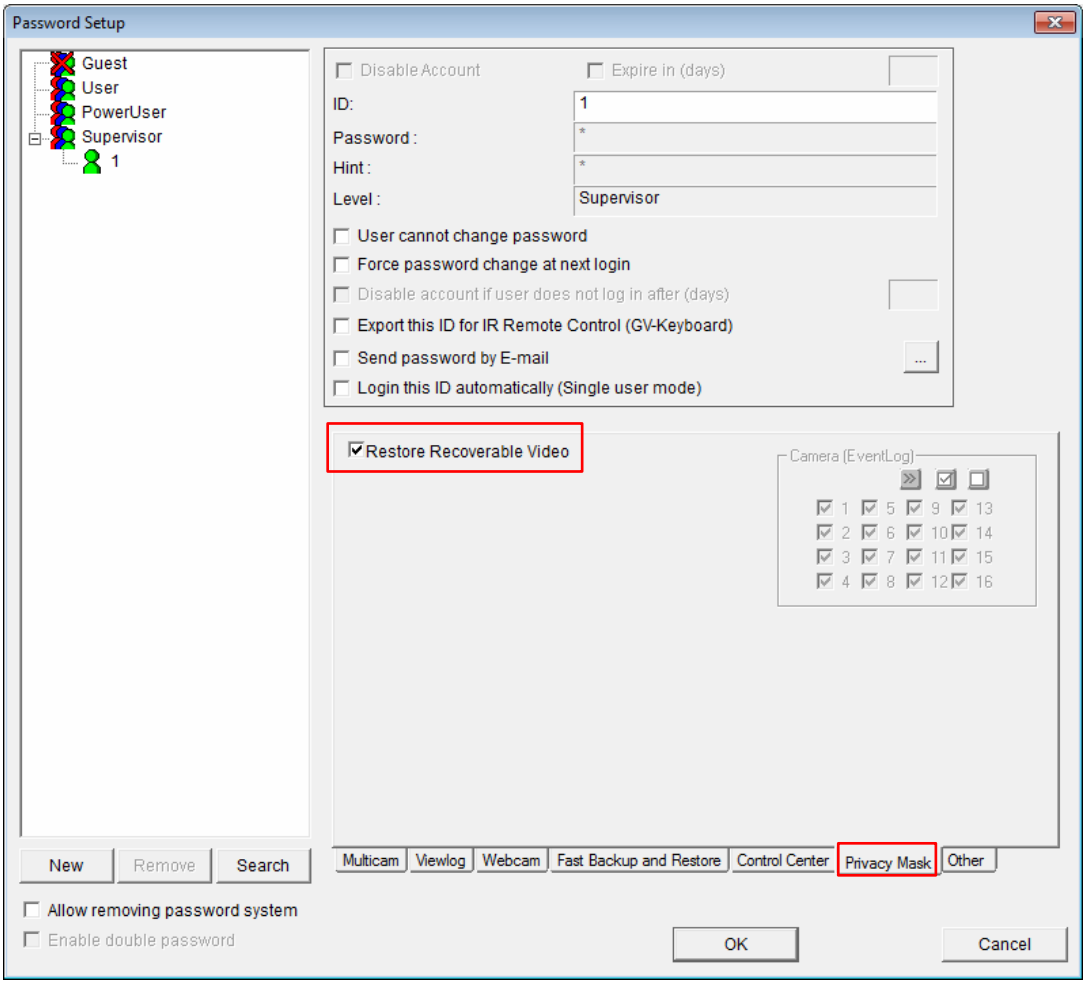


Figure 3-44

Note: If you open the event files (*.avi) directly from local disks, the valid ID and password are also required to access the block-out areas. For more information on retrieving the block-out areas in the exported files, see *Merging and Exporting Video* in Chapter 4.

3.11 Scene Change Detection

The Scene Change Detection can detect when a camera has been tampered physically. This feature can generate an alert whenever someone or something has covered the lens of the camera, or when the camera has been moved, or when it is out of focus.

1. Click the **Configure** button (No. 14, Figure 1-2), select **Video Analysis**, and select **Scene Change Detection Setting**. The Scene Change Detection Setup dialog box appears.
2. Select the desired cameras to be configured, and then click the **Configure** tab. This dialog box appears.

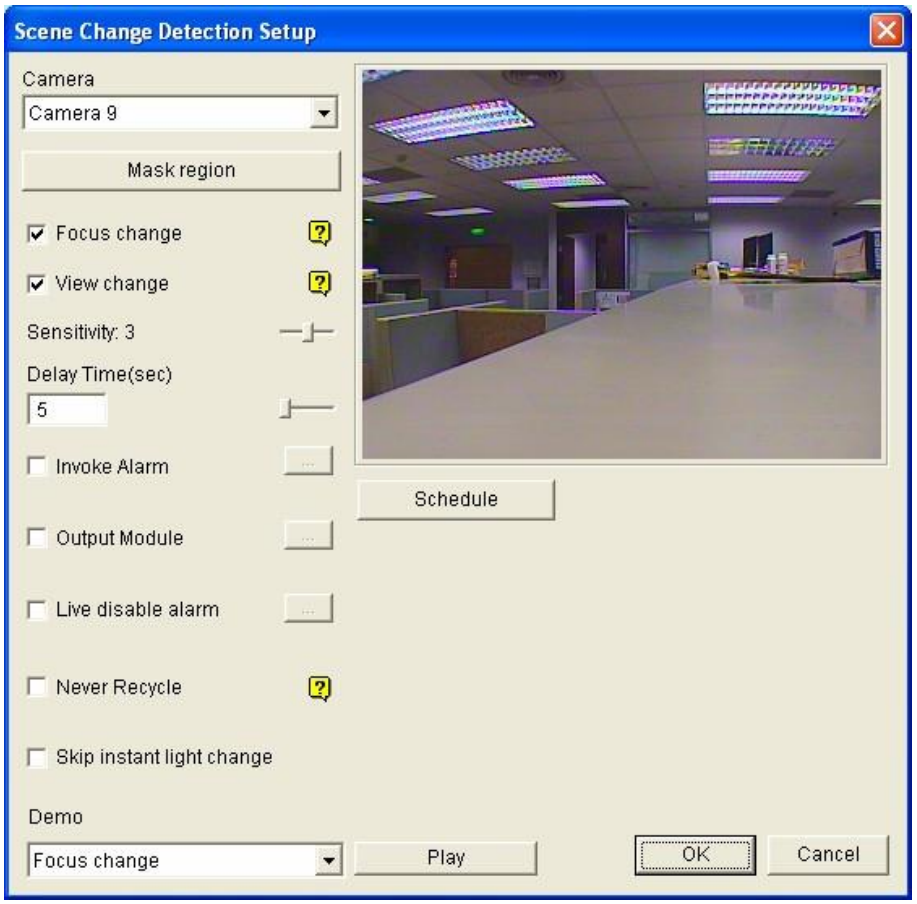


Figure 3-45 *Scene Change Detection Setup*

④ **Camera:** Select the camera to be configured.

④ **Mask region:** Masks off the areas where motion will be ignored.

④ **Focus change:** Generates an alert when the camera is out of focus.

④ **View change:** Generates an alert when the camera has been moved, or the lens of the camera has been covered.

④ **Sensitivity:** Adjusts detection sensitivity. The default value is 3.

④ **Delay Time(s):** Sets the duration of a scene change before an alarm condition is triggered.

④ **Invoke Alarm:** Activates the computer alarm when a scene change is detected. Click the **[…]** button beside to assign a .wav sound file.

④ **Output Module:** Activates the output device when a scene change is detected. Click the **[…]** button beside to assign the output module and pin number.

④ **Live disable alarm:** Choose whether to invoke the warning message when a scene change is detected. Click the **[…]** button beside to display Figure 3-42.

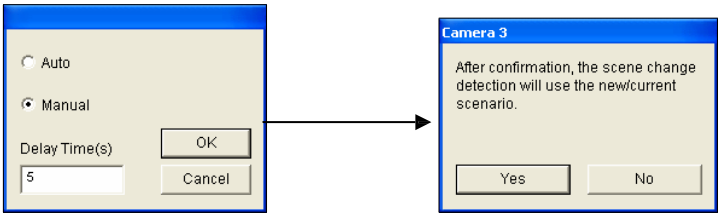


Figure 3-46 ***Figure 3-47***

Select **Auto** to close the warning message (Figure 3-42) automatically or select **Manual** to close it manually. Under **Delay Time(s)**, you can define the duration of a scene change to invoke the message. The range of delay time is from 1 to 99999 seconds.

④ **Never Recycle:** When this option is selected, the event files of scene changes will not be recycled when the recycle threshold is reached.

④ **Demo:** See three examples of Focus Change and View Change. Click the **Play** button to see the demonstration.

④ **Skip Instant Light Change:** Ignores sudden illumination changes and avoids false alarms. For example, light switches can cause illumination changes suddenly. With the option selected, the system will ignore significant illumination changes without triggering the alarm and continue monitoring. See the **Note** in *Crowd Detection* later in this chapter for possible risk.

3. To activate the function at certain times only, click the **Schedule** button and select **Active Schedule**. For details, see *Video Analysis Schedule* later in this chapter.

4. Click **OK** to apply the settings.

5. Start monitoring to run the application.

When a scene change is detected, a warning message will appear on live video (if **Live Disable Alarm** is enabled), the selected alarm or output will be activated, and the event will be recorded as **Scene Change** in System Log for later retrieval.

3.12 Panorama View

A panorama view splices multiple camera images together and allows you to monitor a large area in one view. There are two ways to create a panorama view: Stitching camera images together with overlapping by matching reference points and using the Easy Mode to place camera images next to each other with no overlapping.

The cameras selected for the panorama view will keep the recording in original format. Up to 4 sets of panorama views can be created.

To access this feature, click the **Configure** button (No. 14, Figure 1-2), point to **Advanced Video Analysis**, select **Panorama Setting**, select the desired cameras on be configured, and then click the **Configure** button. This dialog box appears.

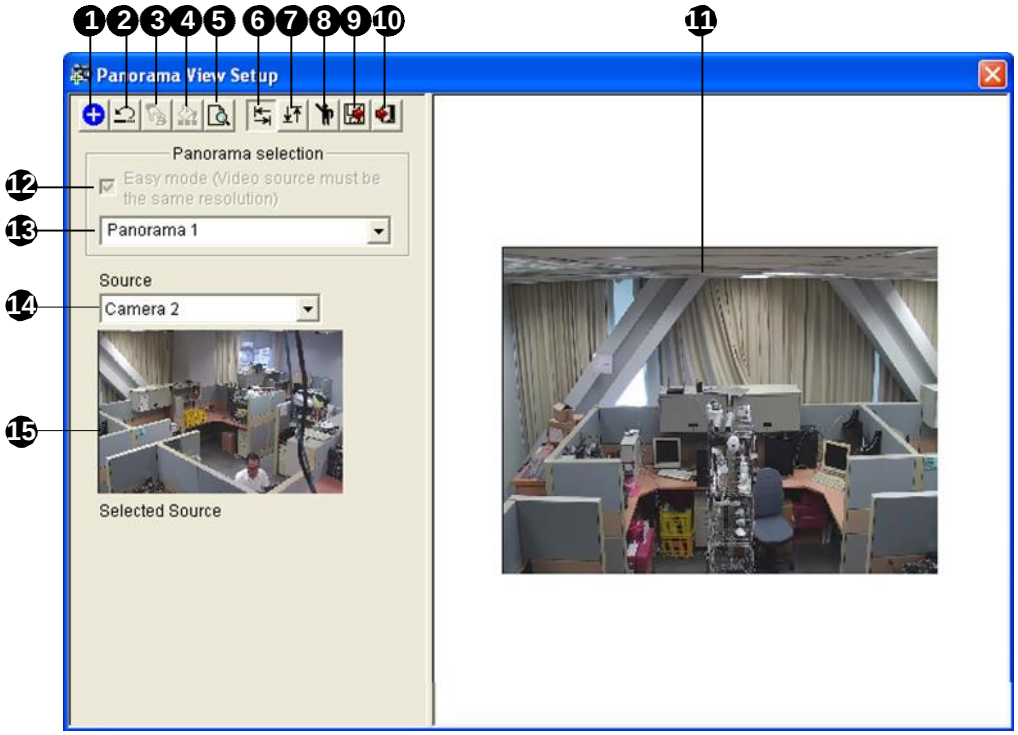


Figure 3-48

The controls on the Panorama View Setup dialog box:

No.	Name	Description
1	Add	Adds an image for automatic splicing.
2	Undo	Cancels the settings.
3	Manual Setting	Manually splices the images together.
4	Blending	Makes the spliced images seamless.
5	Demo	Displays the setup procedure.
6	Left / Right	Place the selected image to the left or right of the previous image.
7	Top / Bottom	Place the selected image on the top or bottom of the previous image.
8	Customize Resolution	Sets the width and height of the panorama view in pixels.
9	Save Before Exit	Saves the created panorama view and closes the dialog box.
10	Exit	Closes the dialog box.
11	Preview Window	Displays the selected source image or the spliced images.
12	Easy Mode	Places camera views next to each other with no overlaps.
13	Panorama Selection	Selects the panorama set for the images to be spliced together. Clicks again to rename the panorama set.
14	Source	Selects the source image to be spliced.
15	Selected Source	Displays the selected image.

3.12.1 Stitching a Panorama View with Overlapping Areas

To stitch images from different cameras together, follow these steps:

1. Select one panorama set (No. 13, Figure 3-48) from the drop-down list. If you want to rename the selected panorama set, type the name in the field.
2. Select one camera from the Source drop-down list (No. 14, Figure 3-48) and then click **Manual Setting** (No.3, Figure 3-48). This dialog box appears.

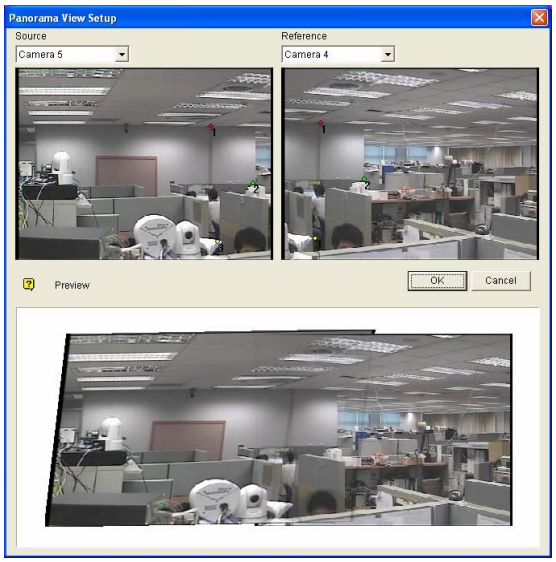


Figure 3-49

3. From the Reference drop-down list, select one camera as the Reference image. At this step, the camera you selected at Step 2 will be the only Reference image.
4. From the Source drop-down list, select one camera as the Source image to be stitched with the selected Reference image.
5. To stitch the two images together, click on a significant point in the Reference image and then look for the same point in the Source image. A dialog box of point selection will prompt you to confirm. You need to set up 3 points for stitching.

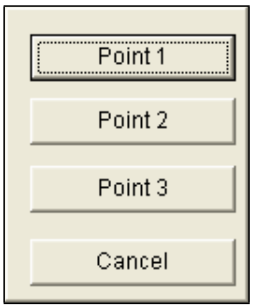


Figure 3-50

Note: For the best result, position the points in the overlapping areas on both images. Avoid placing the points in a cluster or lining them up straight.

6. The resulting image is displayed in the Preview window. If satisfied with the result, click **OK** to exit the setup dialog box. If not, re-enter the 3 points for stitching.
7. If you want to stitch a third image or more, click **Manual Setting** and repeat Steps 3 to 5 multiple times.
8. When you finish stitching images, click the **Save Before Exit** button (No.6, Figure 3-48) to save the created panorama view before exiting the Panorama View Setup dialog box.

Note: The resolution of the images to be stitched will be reduced to 320 x 240. A panorama view has a resolution limit of 1920 x 1080. Once the limit is reached, you cannot stitch more images to the created panorama view.

3.12.2 Easy Mode with No Overlapping Area

When you have multiple camera views covering areas right next to each other with no overlaps, the Easy Mode allows you to simply place camera views together.

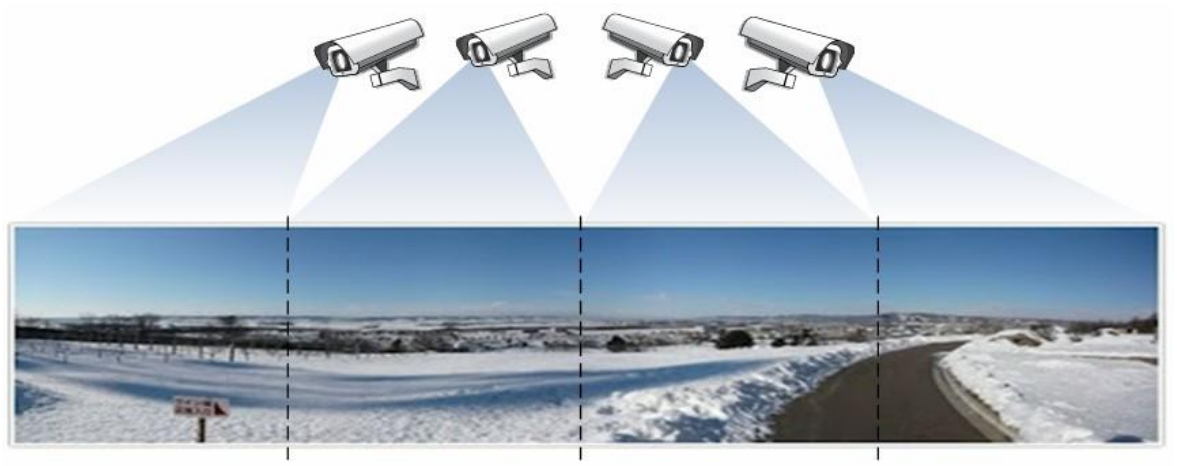


Figure 3-51

1. Select **Easy Mode (Video source must be the same resolution)** (No. 12, Figure 3-48).

2. Use the **Source** drop-down list (No. 14, Figure 3-48) to select the first camera view to be placed in the panorama and click the **Add** button. The first camera view is added to the Preview Window.

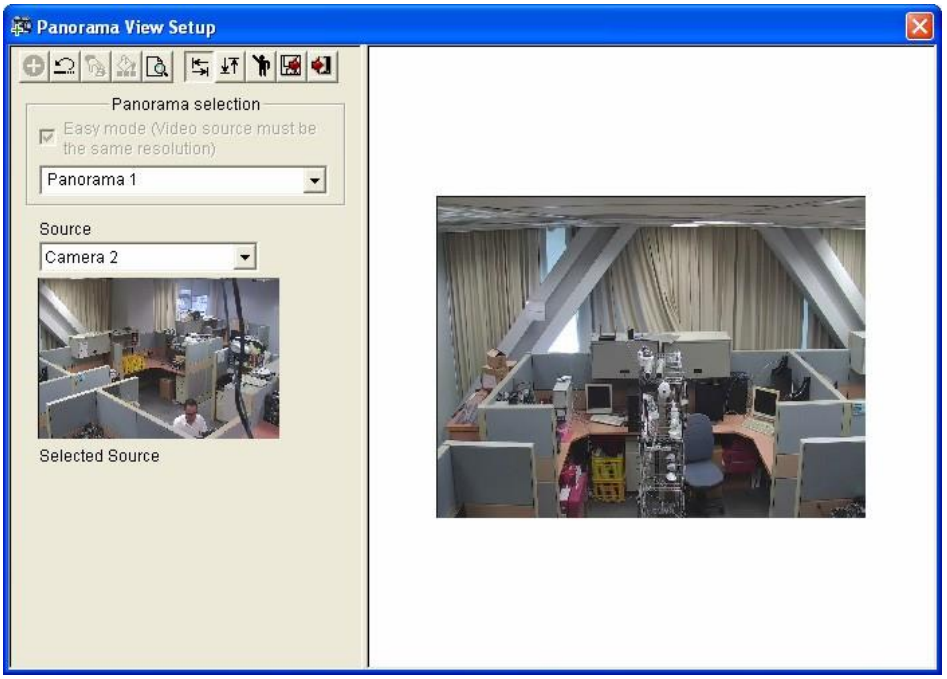


Figure 3-52

3. To add a second camera view, select the camera from the **Source** drop-down list.

4. To place the camera view on the left or right of the first camera view, click the icon and select to place the second view on the **Left** or **Right** of the first view.

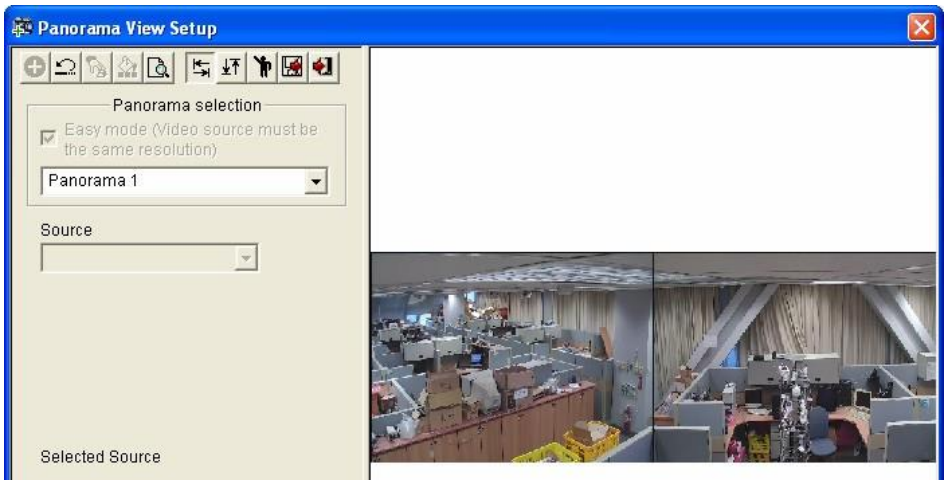


Figure 3-53

5. To place the camera view above or below the first camera view, click the icon and select to place the second view on the **Top** or **Bottom** of the first view.

6. Repeat the steps for any additional cameras.

Note: You will only be able to add additional cameras next to the last camera view added. For example, when adding a third camera, you can only use the direction buttons in relation to the second camera. You will not be able to go back and select the first camera.

7. To specify the width and height of the panorama view, click the **Customize Resolution** icon, select **Enable** and type the **Width** and **Height** in pixels.

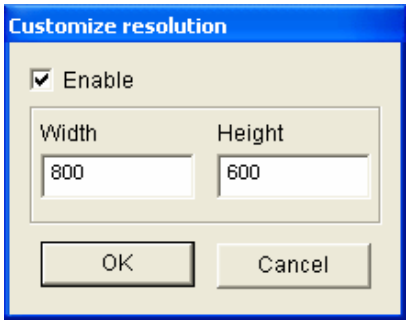


Figure 3-54

8. When you finish stitching images, click the **Save Before Exit** button before exiting.

3.12.3 Accessing a Panorama View

Click the **ViewLog** button (No.13, Figure 1-2), point to **Live Panorama View**, and select the desired panorama set from the list. This window appears.

Figure 3-55

Panorama View Controls

Right-click the panorama view to have these options:

④ **Snapshot:** Save the current panorama view as an image file.

④ **Blending:** Make the two images smoothly blended together. If this is not set, there can be harsh edges in the panorama.

④ **Refresh Rate:** When the panorama view is enabled, the system load will increase. Change the refresh rate for the panorama images to optimize system performance. The refresh rate is from **Speed 1 (Slow)** to **Speed 5 (Fast)**.

④ **PIP View:** Move the navigation box around to have a close-up view of the selected area. See *Picture-in-Picture View* in Chapter 1.

④ **PAP View:** Specify up to 7 close-up views by drawing navigation boxes on the panorama view. See *Picture-and-Picture View* in Chapter 1.

3.13 Video Defogging

Smoky environments and bad weather, such as rain, snow or fog, all affect image quality and reduce scene visibility. This feature helps to enhance image quality for live viewing.

Note: This function takes high CPU and memory usage. Make sure at least 1 GB of RAM is installed on your system.

1. Click the **Configure** button (No. 14, Figure 1-2), select **Advanced Video Analysis**, click **Defog Setting**, select up to 32 cameras to be configured, and then click the **Configure** button. This dialog box appears.

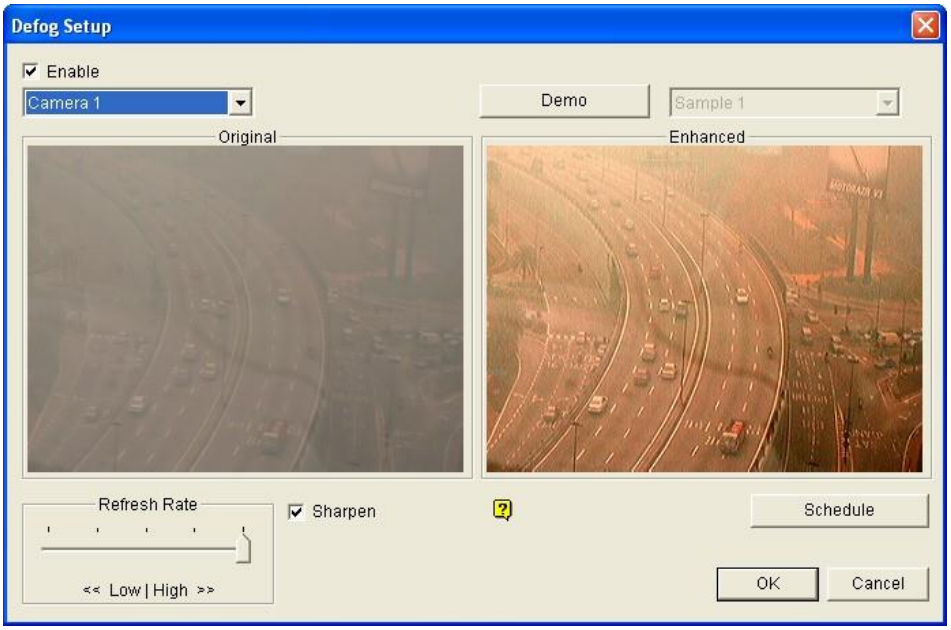


Figure 3-56

2. Use the drop-down list to select a camera and select **Enable**.
3. When the image enhancement is enabled, the system load will increase. Adjust the **Refresh rate** by moving the slide bar to optimize system performance.
4. If you want to view the demonstration of this function, click the **Demo** button.
5. Click **Schedule** to set a schedule to enable the function. For details, see *Video Analysis Schedule* later in this chapter.

Note:

1. This function only applies to live view and does not affect the recorded video, but it can also be applied after a video is recorded. Refer to the *Playing Back on ViewLog* section in Chapter 4 for details.
2. If dual-stream IP channels are applied, for better image quality, it is recommended to change the streaming to single stream before you enable these video analysis effects. This effect does not support On Demand Display for automatic adjustment of live video resolution in single-channel division.

3.14 Video Stabilization

Images from a shaky camera are jittery or blurry. This feature helps to reduce camera shake, leaving you with clear and steady images.

Note: This function takes high CPU and memory usage. Make sure at least 1 GB of RAM is installed on your system.

---

1. Click the **Configure** button (No. 14, Figure 1-2), select **Advanced Video Analysis**, select **Stabilizer Setting**, select up to 4 cameras to be configured, and then click the **Configure** button. This dialog box appears.

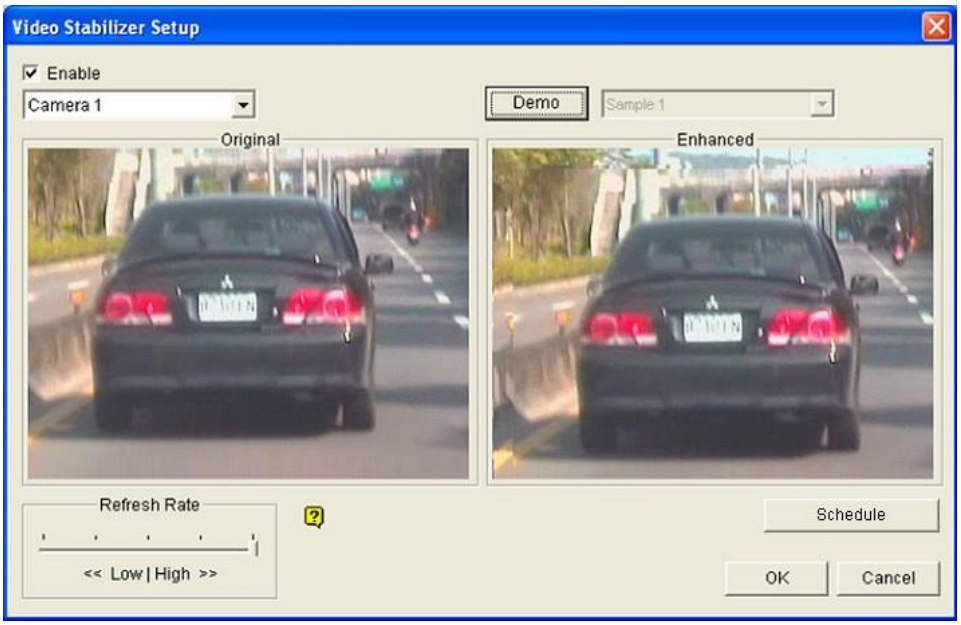


Figure 3-57

2. Use the drop-down list to select one camera, and check the **Enable** option.
3. When the image enhancement is enabled, the system load will increase. Adjust the **Refresh rate** by moving the slide bar to optimize system performance.
4. Click **Schedule** to set a schedule to enable the function. For details, see *Video Analysis Schedule* later in this chapter.
5. If you want to view the demonstration of this function, click the **Demo** button.

Note:

1. This function only applies to live view and does not affect the recorded video, but it can also be applied after a video is recorded. Refer to the *Playing Back on ViewLog* section in Chapter 4 for details.

2. If dual-stream IP channels are applied, for better image quality, it is recommended to change the streaming to single stream before you enable video stabilization. This effect does not support On Demand Display for automatic adjustment of live video resolution in single-channel division.

3.15 Wide Angle Lens Dewarping

Camera images can sometimes appear curved toward the edges of the view. This feature helps correct distortion towards the edge of the camera view.

1. Click the **Configure** button (No. 14, Figure 1-2), select **System Configure** and select **Camera Configure**. This dialog box appears.

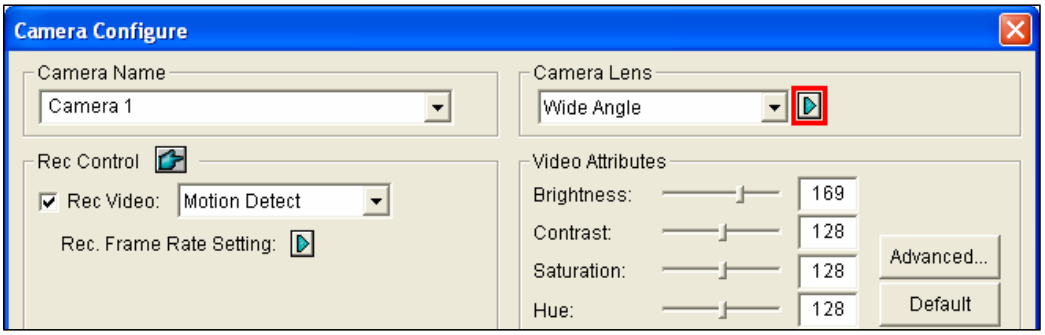


Figure 3-58

2. Use the **Camera Lens** drop-down list to select **Wide Angle**.
3. Click the button. This dialog box appears.

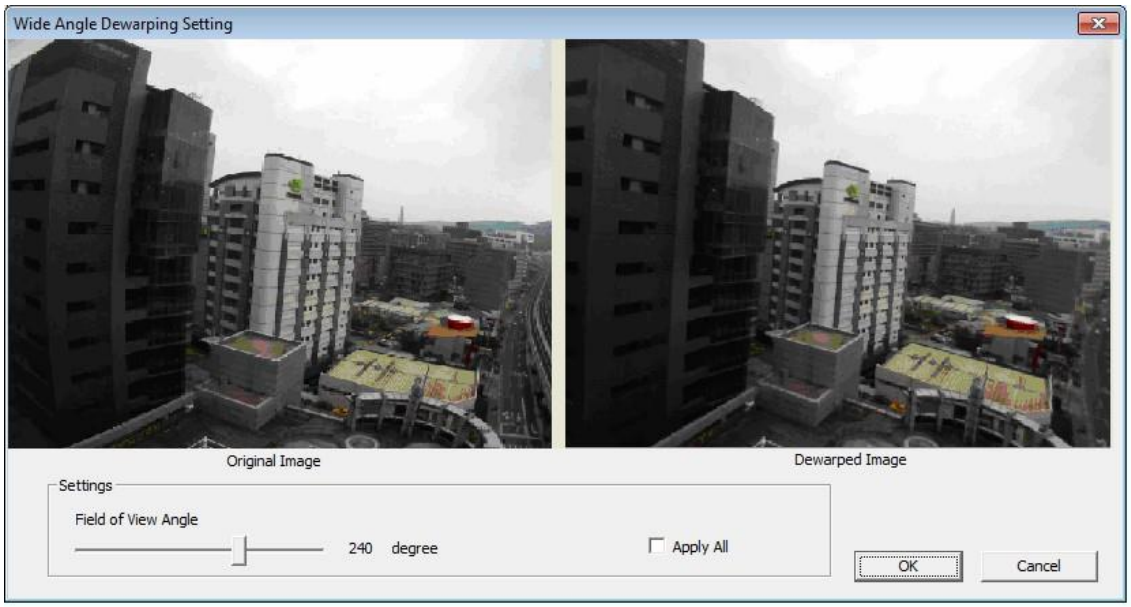


Figure 3-59

4. Move the slider to adjust the degree of warping. The adjusted view is shown on the right.
5. Click **OK**.
6. On the main screen, right-click the live view, select the camera number and select **Wide Angle Lens Dewarping** to apply the setting.

Note:

1. This function only applies to live view and does not affect the recorded video, but it can also be applied after a video is recorded. Refer to the *Adjusting Distorted Views* section in Chapter 4 for details.
2. If dual-stream IP channels are applied, for better image quality, it is recommended to change the streaming to single stream before you enable wide angle lens dewarping. This effect does not support On Demand Display for automatic adjustment of live video resolution in single-channel division.

3.16 Advanced Motion Detection

To avoid false motion detection, the Advanced Motion Detection feature provides five solutions:

- ⌘ Designate up to 5 levels of motion detection sensitivity for each outlined area
- ⌘ Mask off unwanted areas for monitoring, such as cloud and tree movement
- ⌘ Ignore video noise when the lighting condition is poor or changed
- ⌘ Set a minimum and maximum object size to only detect objects within the size range
- ⌘ Ignore environmental changes such as rain, snow and tree movement

Note: You can only enable either motion detection by sensitivity or by object size at a time.

1. Click the **Configure** button (No. 14, Figure 1-2), point to **Video Analysis**, and then select **Advanced Motion Detection Setting**. The Advanced Motion Detection Setup dialog box appears.
2. Select the camera to be configured, and click the **Configure** button. This dialog box appears.

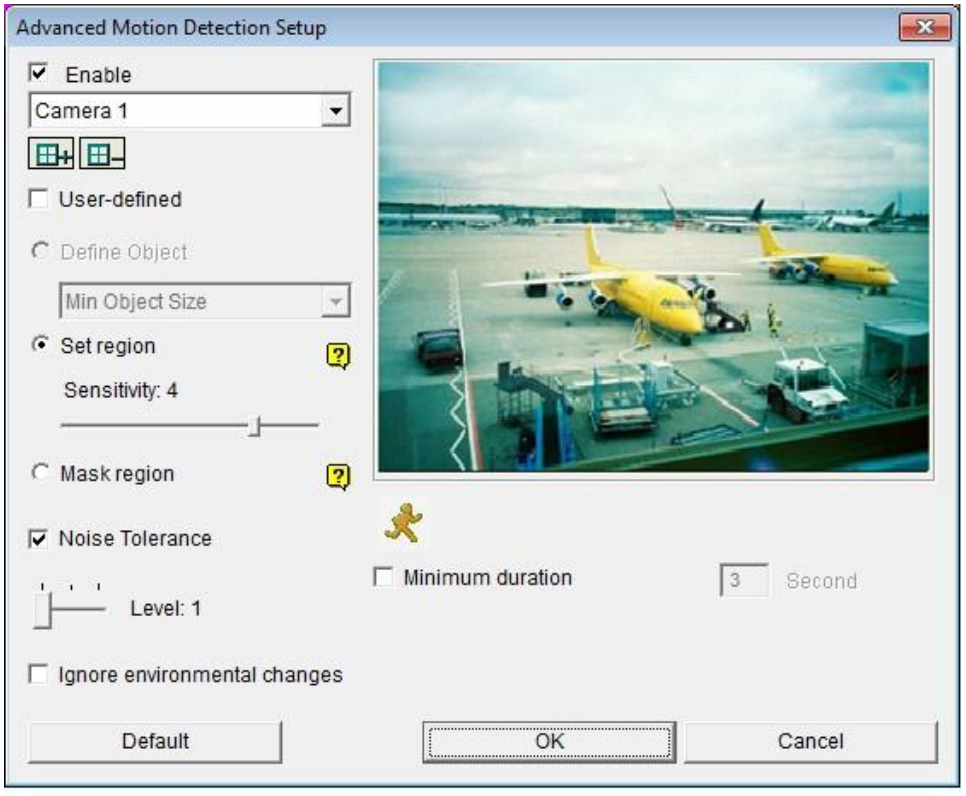


Figure 3-60 *Advanced Motion Detection Setup*

3. Select the desired camera from the drop-down list.

4. To limit motion detection to objects within a size range, select **User-defined** and select **Define Object**. Select **Min. Object Size** or **Max. Object Size** from the drop-down list and then drag an area on the image.
5. To set detection sensitivity in a specific area, clear the selection for **User-defined** and click **Set region**. Select a sensitivity level by moving the slider, and then drag an area on the image. This setup has sensitivity levels from 1 to 5, with 4 as default. You can create several areas with different sensitivity levels.
6. If you want to ignore motion in a certain area, click **Mask Region**, and then drag an area on the image.
7. If you want to ignore video noise when light changes, select **Noise Tolerance** and use the slider to adjust the level. The higher the level, the more tolerant the system is to video noise.
8. If you want to ignore environmental changes such as rain or snow, select **Ignore environmental changes**.
9. To set minimum time for motions to be counted as motion detection, select **Minimum duration** and specify the minimum number of seconds motions must exceed (Max. 60 seconds),
10. Click **OK** to save your settings.

Note:

1. This feature must work with the recording mode of Motion Detection: click the **Configure** button (No. 14, Figure 1-2), point to **System Configure**, select **Camera Configure**, check **Rec Video**, and then select **Motion Detect** (Figure 1-9).
2. If you have set up **Motion Sensitivity** and **Mask Filter** in the Camera Configure settings (Figure 1-10), note that the configurations of Advanced Motion Detection have priority over these settings.
3. When **Ignore environmental changes** is selected, objects moving steadily and repeatedly in the same direction for over 1.5 seconds will be filtered out and ignored.

3.17 Crowd Detection

Crowd detection is used to generate an alert when a crowd of people gathers in a specified area and exceeds the defined time threshold.

Note: Up to 16 cameras can be configured for this application.

---

1. Click the **Configure** button (No. 14, Figure 1-2), click **Advanced Video Analysis**, and select **Crowd Detection Setting**.
2. Select the desired camera(s) to be configured, and click **Configure**. This dialog box appears.

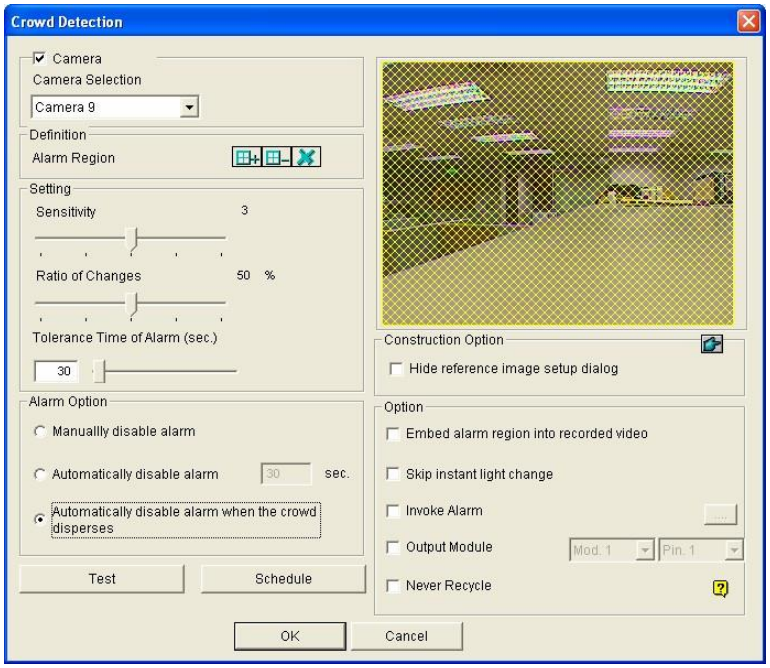


Figure 3-61

3. Select a camera from the Camera Selection drop-down list.
4. By default the whole camera view is set to be the alarm region. Click the button to clear the default setting. Click the button to freely draw the alarm region. To cancel the previously drawn area, click the button.
5. Select **Ratio of Changes**. When the selected ratio of changes in the defined alarm region is detected, the alarm will be activated. The smaller the ratio of changes, the more sensitive the system is for changes in the camera view.
6. Specify **Tolerance Time of Alarm** in seconds that allows a crowd to stay before an alarm condition is activated.

7. Every time when the system detects changes in the background image, you will be prompted for alert. If you want to close the prompt, select **Hide Reference Image Setup Dialog**.
8. In the Options section, you can optionally configure these settings:
    - **Automatically Disable Alarm**: Stops all types of triggered alerts, including computer alarm, flashing boxes and output module after the specified duration. Disabling the alerts will not disable alert settings and the detection in progress.
    - **Embed Alarm Region into Recorded Video:** This option will contain the flashing alert boxes in the recorded files so that you can easily spot suspicious events during playback. Note that if you are used to searching suspicious events with **Object Search**, do not enable this option. These flashing boxes can cause false alarms.
    - **Skip Instant Light Change:** Ignores sudden illumination changes and avoids false alarms. For example, light switches can cause illumination changes suddenly. With the option selected, the system will ignore significant illumination changes without triggering the alarm and continue monitoring. See the **Note** below for possible risk.
    - **Invoke Alarm:** Enables the computer alarm when an assemblage is detected. Click the **[…]** button next to the option to assign a .wav sound file.
    - **Output Module:** Activates the output device when an assemblage is detected. Click the **[…]** button next to the option to assign an installed output module and a pin number.
    - **Never Recycle:** Prevents the system from recycling the event files of crowd detection when the recycle threshold is reached.
9. You can click **Test** to test your settings. If an assemblage cannot be detected, decrease **Ratio of Changes** to increase the system sensitivity for detection.
10. To activate the function at certain times only, click the **Schedule** button and select **Active Schedule**. For details, see *Video Analysis Schedule* later in this chapter.
11. Click **OK** to apply the settings.
12. Start monitoring to run the application.

When a crowd of people gathers in the alarm region for the specified time, its location will be highlighted on live video, the selected alarm or output will be activated, and the event will be recorded as **Crowd Detection** in System Log for later retrieval.

Note:

For the **Skip Instant Light Change** option:

1. When it is selected, you may be subject to the risk that the system will not generate an alert whenever the lens of the camera is covered by malice.
2. If the infrared camera is in use, it is not recommended to select this option.

If you do not select **Automatically Disable Alarm**, you can stop all types of triggered alerts by this step: Right-click on the camera image which has a flashing box indicating a triggered alert, select **Camera**, select **Crowd Detection** and select either **Reset Background Model** or **Reset Alert**.

④ **Reset Background Model:** Rebuilds the reference image and resets the triggered alert. The replaced reference image will be used as the base image for comparison with images on the camera view to detect changes. The system will accept the crowd from this point on and no longer generate any alert for it.

④ **Reset Alert:** Disables and resets the triggered alert. After the alert is reset if the crowd remains gathering over the specified tolerance time, the system will still detect it as a crowd gathering and keep generating alert.

3.18 Advanced Scene Change Detection

Compared to Scene Change Detection that can only be applied in the indoors, the advanced version of Scene Change Detection can be applied in the outdoors. The Advanced Scene Change Detection detects and prevents any changes of scene, viewing angle or focus clearness made by malice.

Note:

1. Up to 16 cameras can be configured for this application.
2. It is highly recommended not to use Advanced Scene Change Detection and Scene Change Detection together.

---

1. Click the **Configure** button (No. 14, Figure 1-2), click **Advanced Video Analysis**, and select **Advanced Scene Change Detection Setting**.
2. Select the desired camera(s) to be configured, and click **Configure**. This dialog box appears.

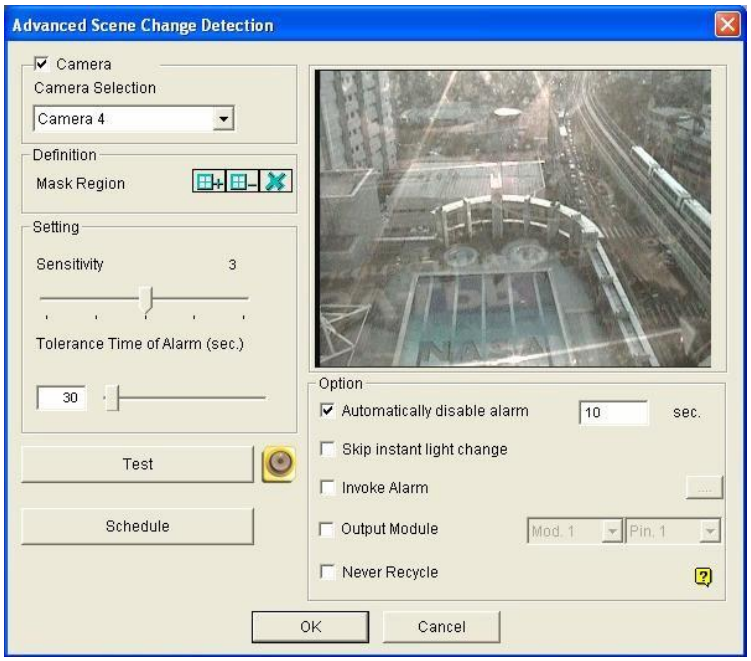


Figure 3-62

3. Select a camera from the Camera Selection drop-down list, and configure these settings:

   ④ **Mask Region:** If necessary, mask off the area on the camera view where motion will be ignored.

   ④ **Sensitivity:** Adjusts detection sensitivity. The higher the value, the more sensitive the system is for changes in the camera view.

- ④ **Tolerance Time of Alarm:** Sets the duration of scene change before an alarm condition is activated.
- ④ **Automatically Disable Alarm**: Stops all types of triggered alerts, including sound alarm, flashing boxes and output module after the specified duration. Disabling the alerts will not disable alert settings and the detection in progress.
- ④ **Skip Instant Light Change:** Ignores sudden illumination changes and avoids false alarms. For example, light switches can cause illumination changes suddenly. With the option selected, the system will ignore significant illumination changes without triggering the alarm and continue monitoring. See the **Note** in *Crowd Detection* earlier in this chapter for possible risk.
- ④ **Invoke Alarm:** Enables the computer alarm when the scene change is detected. Click the **[…]** button next to the option to assign a .wav sound file.
- ④ **Output Module:** Activates the output device when the scene change is detected. Click the **[…]** button next to the option to assign an installed output module and a pin number.
- ④ **Never Recycle:** Prevents the system from recycling the event files of scene change when the recycle threshold is reached.

4. You can click **Test** to test your settings. If the scene change cannot be detected, increase **Sensitivity** value to increase system sensitivity to changes in the camera view.
5. To activate the function at certain times only, click the **Schedule** button and select **Active Schedule**. For details, see *Video Analysis Schedule* later in this chapter.
6. Click **OK** to apply the settings.
7. Start monitoring to run the application.

When a scene change is detected in the camera view for the specified time, its location will be highlighted in live video, the selected alarm or output will be activated, and the event will be recorded as **Advanced Scene Change** in System Log for later retrieval.

If you do not select **Automatically Disable Alarm**, you can stop all types of triggered alerts by this step:

Right-click on the camera image which has a flashing box indicating a triggered alert, select **Camera**, select **Advanced Scene Change Detection** and select either **Reset Background Model** or **Reset Alert**.

④ **Reset Background Model:** Rebuilds the reference image and resets the triggered alert. The replaced reference image will be used as the base image for comparison with images on the camera view to detect changes. The system will accept the scene change from this point on and no longer generate any alert for it.

④ **Reset Alert:** Disables and resets the triggered alert. After the alert is reset, if the scene change remains over the specified tolerance time, the system will still detect it as a scene change and keep generating alert.

3.19 Advanced Unattended Object Detection

Compared to Unattended Object Detection that can only be applied in the indoors, the advanced version of Unattended Object Detection can be applied in the outdoors. The Advanced Unattended Object Detection can generate an alert when any unattended object stays within the camera view.

Note:

1. Up to 16 cameras can be configured for this application.
2. It is highly recommended not to use Advanced Unattended Object Detection and Unattended Object Detection together.

---

1. Click the **Configure** button (No. 14, Figure 1-2), click **Advanced Video Analysis**, and select **Advanced Unattended Object Detection Setting**.
2. Select the desired camera(s) to be configured, and click **Configure**. This dialog box appears.

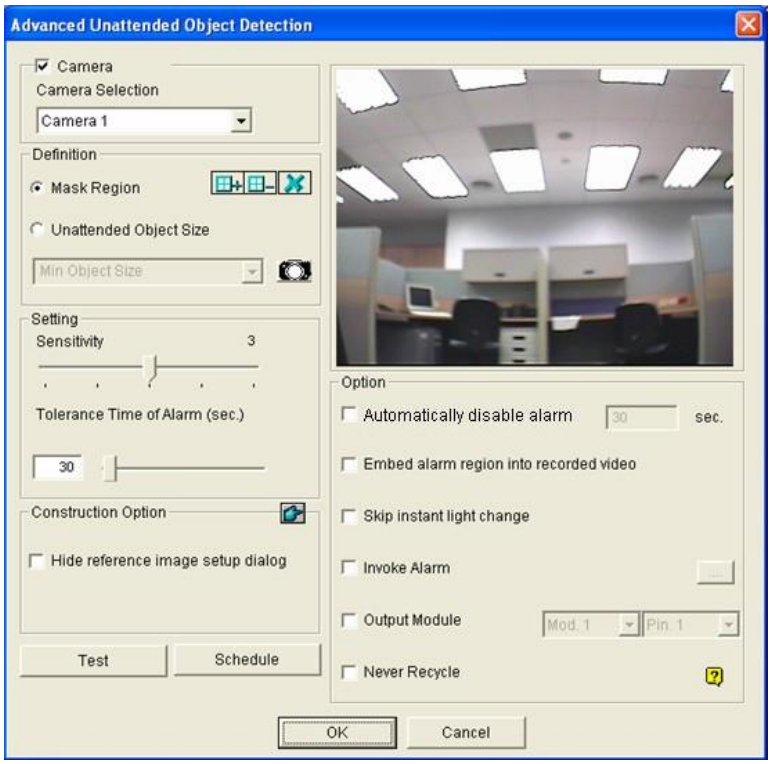


Figure 3-63

3. Select a camera from the Camera Selection drop-down list.
4. If necessary, use the **Mask Region** function to mask off the area on the camera view where motion will be ignored.
5. Select **Unattended Object Size**, and click the Camera icon to pause live images.

6. Outline **Min Object Size** on the camera view, and select **Max Object Size** from the drop-down list and outline it on the camera view.
7. Select **Sensitivity**. The higher the value, the more sensitive the system is for changes in the camera view.
8. Specify **Tolerance Time of Alarm** in seconds that allows any unattended object to stay before an alarm condition is activated.
9. Every time when the system detects changes in the background image, you will be prompted for alert. If you want to close the prompt, select **Hide Reference Image Setup Dialog**.
10. In the Options section, configure these settings:
    - **Automatically Disable Alarm**: Stops all types of triggered alerts, including computer alarm, flashing boxes and output module after the specified duration. Disabling the alerts will not disable alert settings and the detection in progress.
    - **Embed Alarm Region into Recorded Video:** This option will contain the flashing alert boxes in the recorded files so that you can easily spot suspicious events during playback. Note that if you are used to searching suspicious events with **Object Search**, do not enable this option. These flashing boxes can cause false alarms.
    - **Skip Instant Light Change:** Ignores sudden illumination changes and avoids false alarms. For example, light switches can cause illumination changes suddenly. With the option selected, the system will ignore significant illumination changes without triggering the alarm and continue monitoring. See the **Note** in *Crowd Detection* earlier in this chapter for possible risk.
    - **Invoke Alarm:** Enables the computer alarm when an unattended object is detected. Click the **[…]** button next to the option to assign a .wav sound file.
    - **Output Module:** Enables the output device when an unattended object is detected. Click the **[…]** button next to the option to assign an installed output module and a pin number.
    - **Never Recycle:** With the option selected, the event files of unattended object detection will not be recycled when the recycle threshold is reached.
11. You can click **Test** to test your settings. If the unattended object cannot be detected, increase **Sensitivity** value to increase system sensitivity to changes in the camera view.
12. To activate the function at certain times only, click the **Schedule** button and select **Active Schedule**. For details, see *Video Analysis Schedule* later in this chapter.
13. Click **OK** to apply the settings
14. Start monitoring to run the application.

When any unattended object is detected in the camera view for the specified time, its location will be highlighted in live video, the selected alarm or output will be activated, and the event will be recorded as **Advanced Unattended Object** in System Log for later retrieval.

If you do not select **Automatically Disable Alarm**, you can stop all types of triggered alerts by this step: Right-click on the camera image which has a flashing box indicating a triggered alert, select **Camera**, select **Advanced Unattended Object Detection** and select either **Reset Background Model** or **Reset Alert**.

④ **Reset Background Model:** Rebuilds the reference image and resets the triggered alert. The replaced reference image will be used as the base image for comparison with images on the camera view to detect changes. The system will accept the unattended object from this point on and no longer generate any alert for it.

④ **Reset Alert:** Disables and resets the triggered alert. After the alert is reset if the object remains unattended over the specified tolerance time, the system will still detect it as an unattended object and keep generating alert.

.

3.20 Advanced Missing Object Detection

Compared to Missing Object Detection that can only be applied in the indoors, the advanced version of Missing Object Detection can be applied in the outdoors. The Advanced Missing Object Detection can generate an alert when any object disappears from the camera view.

Note:

1. Up to 16 cameras can be configured for this application.
2. It is highly recommended not to use Advanced Missing Object Detection and Missing Object Detection together.

---

1. Click the **Configure** button (No. 14, Figure 1-2), click **Advanced Video Analysis**, and select **Advanced Missing Object Detection Setting**.
2. Select the desired camera(s) to be configured, and click **Configure**. This dialog box appears.

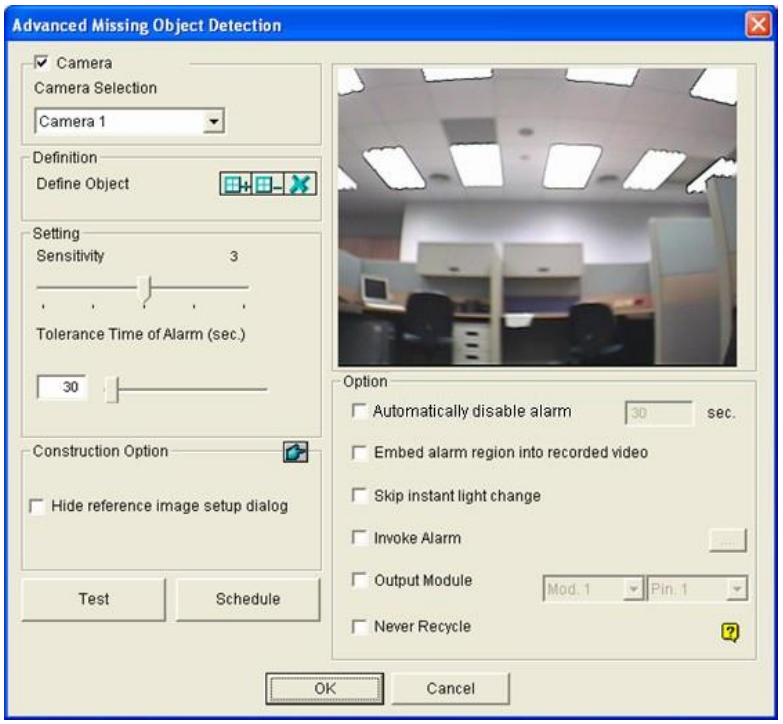


Figure 3-64

3. Select a camera from the Camera Selection drop-down list.
4. Click the button to outline the regions on the objects you want to detect. To cancel the previously drawn area, click the button.
5. Select **Sensitivity**. The higher the value, the more sensitive the system is for changes in the camera view.

6. Specify **Tolerance Time of Alarm** in seconds that allows any object missing before an alarm condition is activated.
7. Every time when the system detects changes in the background image, you will be prompted for alert. You can disable the prompt by selecting **Hide Reference Image Setup Dialog**.
8. In the Options section, configure these settings:
   - ④ **Automatically Disable Alarm:** Stops all types of triggered alerts, including sound alarm, flashing boxes and output module after the specified duration. Disabling the alerts will not disable alert settings and the detection in progress.
   - ④ **Embed Alarm Region into Recorded Video:** This option will contain the flashing alert boxes in the recorded files so that you can easily spot suspicious events during playback. Note that if you are used to searching suspicious events with **Object Search**, do not enable this option. These flashing boxes can cause false alarms.
   - ④ **Skip Instant Light Change:** Ignores sudden illumination changes to avoid false alarms. For example, light switches can cause illumination changes suddenly. With the option selected, the system will ignore significant illumination changes and continue monitoring. See the **Note** in *Crowd Detection* earlier in this chapter.
   - ④ **Invoke Alarm:** Enables the computer alarm when an object is detected to be missing. Click the **[…]** button next to the option to assign a .wav sound file.
   - ④ **Output Module:** Enables the output device when an object is detected to be missing. Click the **[…]** button next to the option to assign an installed output module and a pin number.
   - ④ **Never Recycle:** With the option selected, the event files of missing object detection will not be recycled when the recycle threshold is reached.
9. You can click **Test** to test your settings. If the missing object cannot be detected, increase **Sensitivity** value to increase system sensitivity to changes in the camera view.
10. To activate the function at certain times only, click the **Schedule** button and select **Active Schedule**. For details, see *Video Analysis Schedule* later in this chapter.
11. Click **OK** to apply the settings.
12. Start monitoring to run the application.

When any object, which you have outlined the regions for, disappears from the camera view for the specified time, its location will be highlighted in live video, the selected alarm or output will be activated, and the event will be recorded as **Advanced Missing Object** in System Log for later retrieval.

If you do not select **Automatically Disable Alarm**, you can stop all types of triggered alerts by this step:

Right-click on the camera image which has a flashing box indicating a triggered alert, select **Camera**, select **Advanced Missing Object Detection** and select either **Reset Background Model** or **Reset Alert**.

④ **Reset Background Model:** Rebuilds the reference image and resets the triggered alert. The replaced reference image will be used as the base image for comparison with images on the camera view to detect changes. The system will accept the object missing from this point on and no longer generate any alert for it.

④ **Reset Alert:** Disables and resets the triggered alert. After the alert is reset if the object remains missing over the specified tolerance time, the system will still detect it as a missing object and keep generating alert.

3.21 Video Analysis Schedule

A schedule monitoring has been added to most of **Advanced Video Analysis** and **Video Analysis** functions. This feature allows you to maximize the use of cameras and video analysis effects on each camera. With this feature, you can set multiple video analysis effects on each camera at different times.

For example, previously when you want to configure **Counter Setting** to count the number of people during work hours and also configure **Intrusion Alarm Setting** for thief detection after work hours, you will require 2 cameras at the same location for this scenario. But with the feature, you can set a schedule with just 1 camera to do **Counter Setting** between 7AM-5PM (working hours) and **Intrusion Alarm Setting** between 5PM-7AM (after work hours).

Only a few functions of video analysis do not support the schedule feature. These functions are **Camera Popup Setting**, **Advanced Motion Detection**, **Video Lowpass Filter Setting** and **Panorama Setting**.

To set the Video Analytic schedule:

1. Click the **Configure** (No. 14, Figure 1-2) button, select **Video Analysis** or **Advanced Video Analysis**, select a supported analysis function, select the cameras to be configured and click **Configure**. For this example, **Counter/Intrusion Alarm Setting** is selected and this dialog box appears.

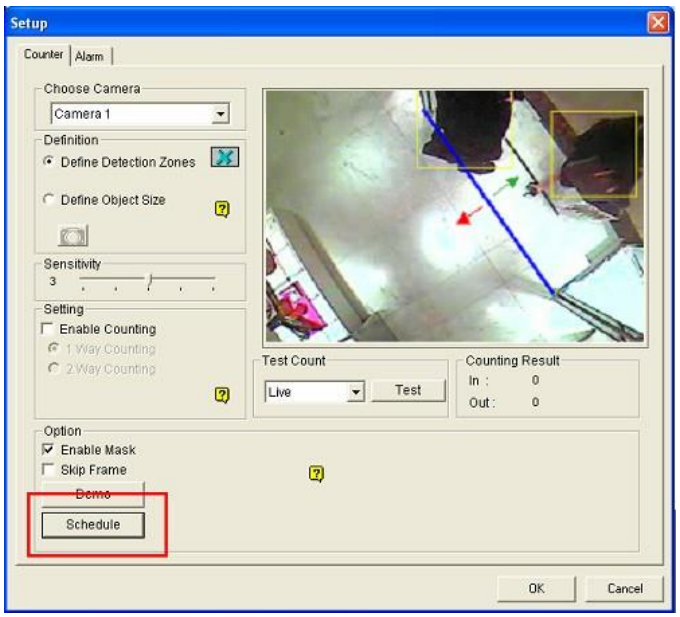


Figure 3-65

2. Click the **Schedule** button in the bottom left corner of the dialog box. This dialog box appears.

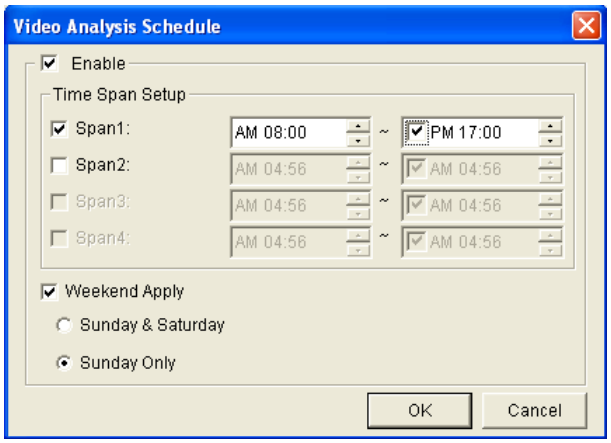


Figure 3-66

3. Select **Enable** to apply video analytic schedule.
4. Select **Span 1** and specify a time period. The period that you specify is effective from Monday through Sunday.
5. Set more spans based on your requirements.
6. To have the video analysis function all day on the weekend, select **Weekend Apply** and define whether the weekend includes **Sunday & Saturday** or **Sunday Only**.
7. Click **OK** to apply the settings.

3.21.1 Privacy Mask Schedule

The schedule setting of Privacy Mask allows you to disable the function during holidays and weekends.

1. Click the **Configure** (No. 14, Figure 1-2) button, select **Video Analysis**, select **Privacy Mask Setting**, select the cameras to be configured and click **Configure**.
2. Click the **Schedule** button.

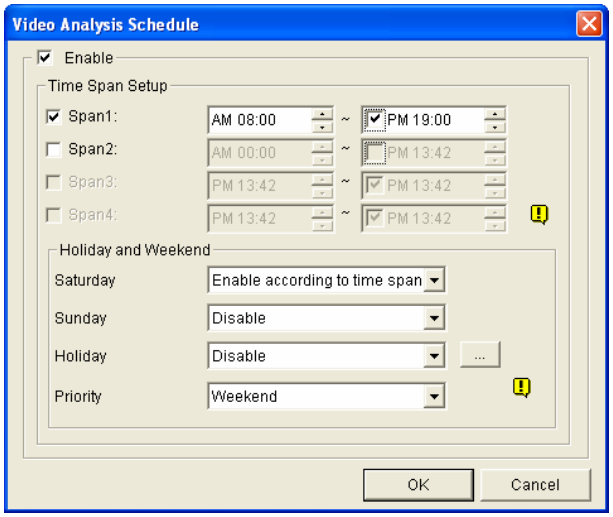


Figure 3-67

3. Select **Enable** to enable video analytic schedule.
4. Select **Span 1** and specify a time period. The period that you specify is effective from Monday through Friday.
5. Set more spans based on your needs.
6. Set the schedule for holidays and weekends by selecting **Enable according to time span**, **Enable all day** or **Disable**.
7. Use the **Priority** drop-down list to select whether to use the schedule setting for **Holiday** or **Weekend** when the holiday is on a weekend.
8. Click **OK** to apply the settings.

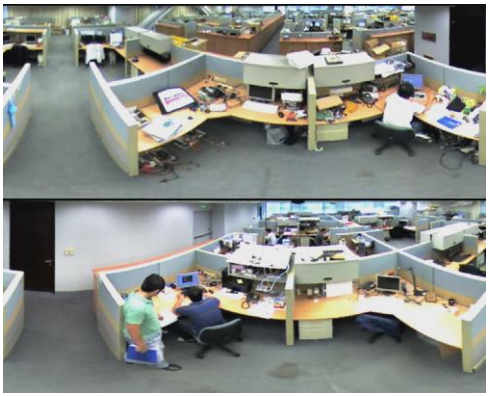
3.22 Fisheye View

A fisheye camera allows you to cover all angles of a location with just one fisheye camera. The distorted hemispherical image produced by the fisheye camera will be converted to a conventional rectilinear projection.

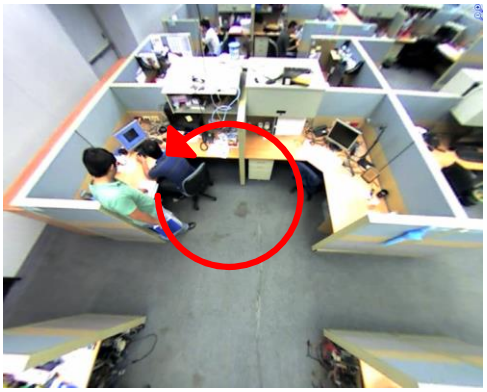
You can choose among four view modes and adjust the PTZ views to different angles.

Quad view: 4 PTZ views

360 degree: 2 PTZ view & 1 360º view



Dual 180 degree: 2 180º views



Single view: 1 PTZ view

Figure 3-68

3.22.1 Setting Up a -Fisheye Camera

1. Right-click the image of the fisheye camera, select the camera number, and select **Geo Fisheye**.
2. To customize the fisheye settings, right-click the image and select **Fisheye Option**. The following configurations are available:

    - **Camera Modes:** You can choose among four view modes.
        - **Geo Fisheye: Quad view:** Composed of four PTZ views.
        - **Geo Fisheye: 360 degree:** Composed of two PTZ views and one 360º panoramic view.
        - **Geo Fisheye: Dual 180 degree:** Composed of two 180º views.
        - **Geo Fisheye: Single view:** Composed of one PTZ view. This view mode supports the advanced Picture-in-Picture (PIP) function, which allows you to have a close-up dewarped image within the surveillance area without missing the entire view.
        - **Camera Position:** Select **Ceiling**, **Wall** or **Ground** according to where the camera is mounted.
    - **Adjust Auto Pan Speed At Top-Left Channel:** Select low, medium, or high speed to enable Auto Pan for one PTZ view at the rotation speed of your choice. This option applies to **Quad view**, **360 degree** and **Single view**.
    - **Zoom:** Select **Zoom In** or **Zoom Out** and then click on the image.
    - **Show Source Video At Top-Right Channel:** You can display the circular source image in the top-right quadrant when **Quad view** is selected.
    - **Fisheye Settings:**

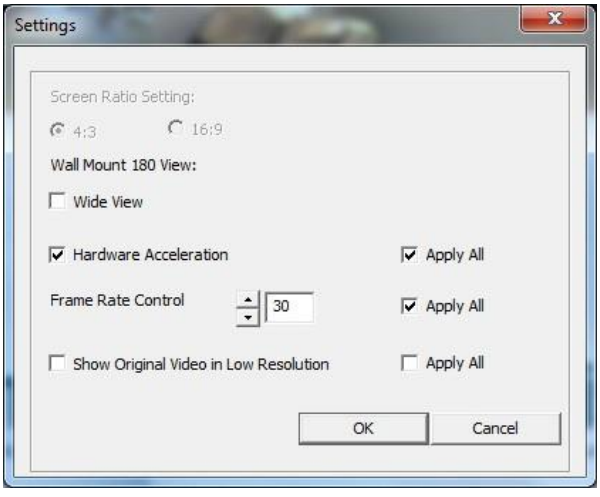


Figure 3-69

- **Screen Ratio Setting:** Sets the display ratio to be **4:3** or **16:9**.
- **Wide View:** Increases the height of the 180 degree view when camera position is set to wall mount.

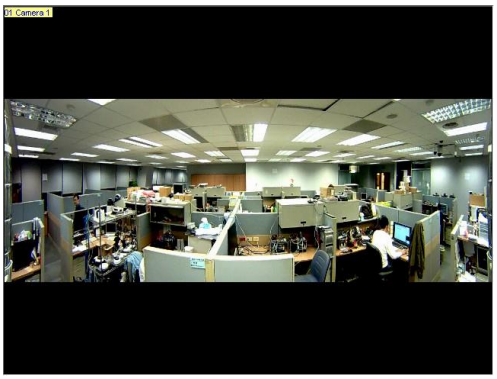


Figure 3-70: Wide View Disabled

Figure 3-71: Wide View Enabled

- **Hardware Acceleration:** Dewarps fisheye view processed by GPU to lower CPU loading. Select **Apply All** to apply the hardware acceleration to other fisheye views.
- **Frame Rate Control:** Limits the frame rate of the fisheye live view to the number specified here. Select **Apply All** to apply the frame rate control to other fisheye views.
- **Show Original Video in Low Resolution:** Shows source video when resolution is low.

Note: The default setting for **Hardware Acceleration** is enabled for GPU dewarping and it automatically detects the Screen Ratio Setting. If you clear **Hardware Acceleration**, it changes to CPU dewarping and you can select the Screen Ratio Setting.

---

3. You can drag and drop PTZ view or 180 degree view to adjust the viewing angle.

3.22.2 Setting Up a Third-Party Fisheye Camera

You can also enable dewarping for 3rd party fisheye cameras and access fisheye related functions.

1. To set up a third-party fisheye camera, click the **Configure** button, select **System Configure** and select **Camera Configure**.

   ⌘ To set up a camera installed with an ImmerVision IMV1 Panorama Lens, under **Camera Lens**, select **IMV1 Panomorph**. On the main screen, click the camera number and select **IMV1 Panomorph** to dewarp images. For details see .Step 2 in *Setting Up a -Fisheye Camera* earlier in this chapter.

   ⌘ For other third-party fisheye cameras, under **Camera Lens**, select **Fisheye**. On the main screen, click the camera number and select **Fisheye** to dewarp images. For details see .Step 2 in *Setting Up a -Fisheye Camera* earlier in this chapter.

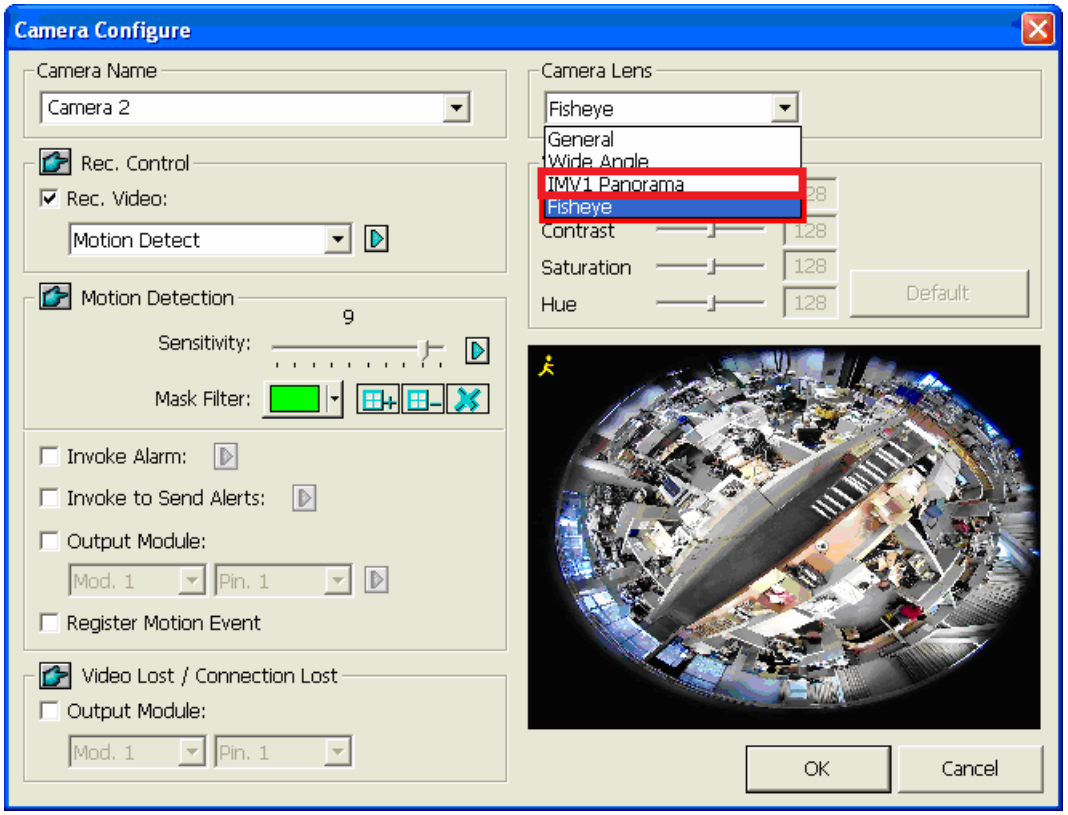


Figure 3-72

2. To adjust the image alignment for optimal results, right-click the camera image, select **Fisheye Option** and select **Image Alignment**. In the dialog box, align the dotted circle with the outer edge of the camera image, and then align it with the inner edge of the image frame.

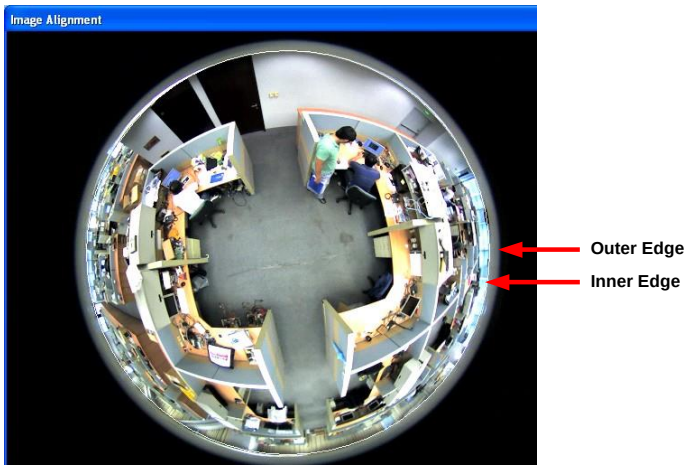


Figure 3-73

3. . To access fisheye related functions, right-click the camera image and select **Fisheye Option**.

Note:

1. For -Fisheye Cameras, the image alignment function is only available on its Web interface.
2. Regardless of the view mode selected here, the hemispherical fisheye source image will be recorded. When playing back the events in ViewLog, the -System will reconvert the source image to different view modes according to your preference. To see how to play back the events in fisheye view mode, see *Playback Screen Layout* in Chapter 4.
3. To enable fisheye functions through WebCam Server, you must first set the fisheye view to megapixel resolution in WebCam settings. Refer to *Hardware-Compressed or Megapixel Stream* in Chapter 8 for more details.

3.22.3 Object Tracking

You can now set up object tracking in fisheye live view to track moving object. The function is only available when the fisheye camera mode is set to be **Geo Fisheye: 360 degree**. When motion is detected in the fisheye, the top-right channel will start tracking the moving object and in the 360 degree view at the bottom, the moving object will be highlighted.

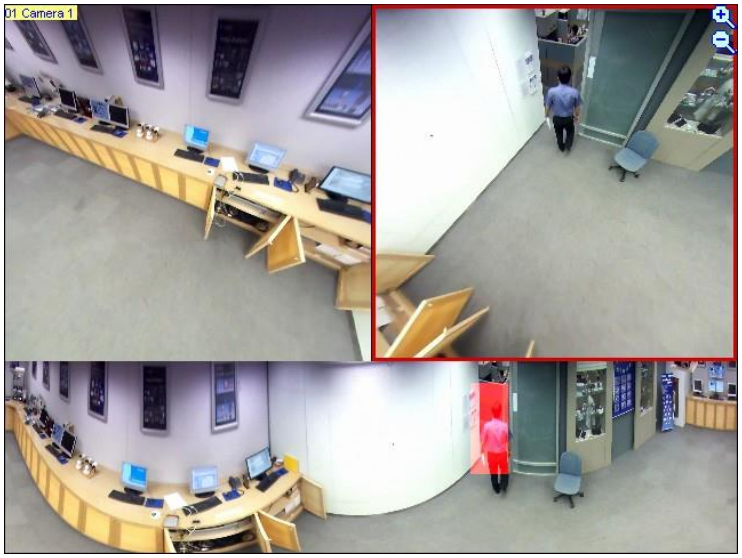


Figure 3-74

2. Right-click the fisheye view, select the camera number and select **Geo Fisheye**.
3. Right-click the fisheye view, select **Fisheye Option**, select **Camera Mode** and select **Geo Fisheye: 360 degree**.
4. Right-click the fisheye view, select **Fisheye Option**, select **360 Object Tracking** and select **Advanced Settings**. This dialog box appears.

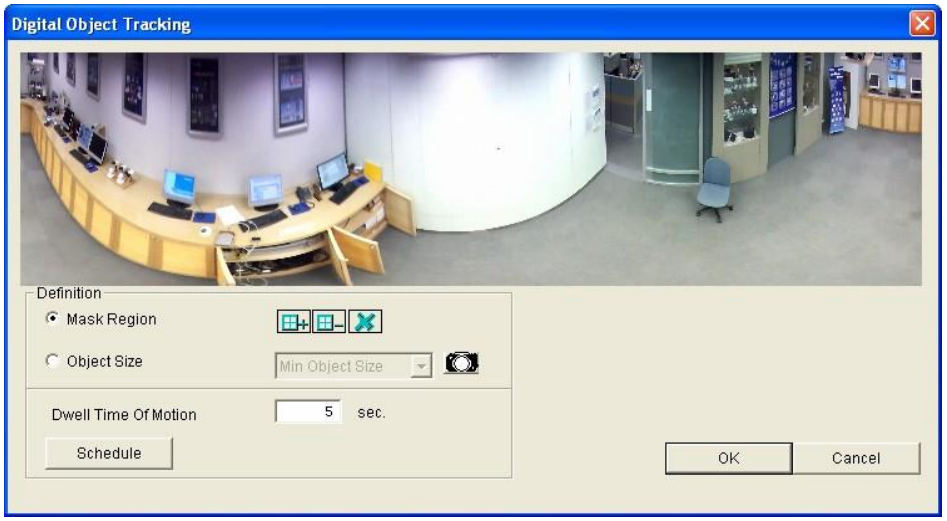


Figure 3-75

5. Use the options below to customize object tracking.
   - ④ **Mask Region:** Use the mouse to outline a mask region where motion will be ignored.
   - ④ **Object Size:** Click the button to pause the live view and then use the mouse to outline the maximum and minimum size of the targeted object.
   - ④ **Dwell Time of Motion:** After a targeted object stops moving, the highlighted region and the top-right channel will remain fixed on the area for the number of seconds specified. Any new motion detected during the dwell time will be ignored to prevent the camera view from frequently jumping from one area to another.
   - ④ **Schedule:** Click **Schedule** to activate object tracking at certain times only. Refer to *Video Analysis Schedule* earlier in this chapter for more details.
6. Right-click the fisheye view, select **Fisheye Option**, select **360 Object Tracking** and select **Tracking** to enable object tracking.

3.23 Specifications

Feature	Notes
Panorama View	⌘ 1 GB of RAM minimum required ⌘ 4 sets of panorama view for live view monitoring
Defogging	⌘ 9 MB of RAM minimum required for each channel ⌘ Maximum of 32 channels
Stabilizer	⌘ 6 MB of RAM minimum required for each channel ⌘ Maximum of 4 channels
Crowd Detection	⌘ Maximum of 16 channels
Advanced Scene Change Detection / Advanced Unattended Object Detection / Advanced Missing Object Detection	⌘ Maximum of 16 channels
Scene Change Detection	⌘ 3 MB of RAM minimum required for each channel
Object Counting	⌘ 7 fps and 9 MB of RAM minimum required for each channel ⌘ Maximum of 16 channels ⌘ 512 MB of RAM and Pentium 4 Dual Core 2.13 GHz of CPU required for 8 or more cameras
Privacy Mask	⌘ 3 MB of RAM minimum required for each channel ⌘ Maximum of 250 detection boxes can be set ⌘ The overall size of detection boxes cannot exceed 102400 bytes.
Face Count	⌘ Maximum of 16 channels
Object Index / Object Monitor / Face Detection /	⌘ 7 fps and 14 MB of RAM minimum required for each channel ⌘ Maximum of 16 channels

Specifications are subject to change without notice.

Note: To use two or more of the following functions simultaneously, at least 2 GB of RAM is required: Advanced Video Analysis, Video Analysis, IP Camera and Pre-Record by Memory.

Chapter 4

Video Playback..... 232

4.1 Playing Back on ViewLog 233

4.1.1 Playback Screen Layout 236

4.1.2 Playback Control Buttons 238

4.1.3 Recycling Option for Video Files 240

4.1.4 Bookmarking a Frame 241

4.1.5 Searching a Video Event 243

4.1.6 Merging and Exporting Video 248

4.1.7 Extracting Frames from a Video Event 255

4.1.8 Saving Images 256

4.1.9 Printing Images 257

4.1.10 Setting Face Mask 259

4.1.11 Displaying GPS Data 261

4.1.12 Adjusting Distorted Views 262

4.1.13 Object Tracking in Fisheye View 263

4.1.14 Event Search Limitation 265

4.1.15 Advanced Settings 266

4.2 Object Search 274

4.3 Advanced Log Browser 277

4.3.1 Filter Settings 279

4.4 Quick Search 281

4.4.1 Event Query Settings 283

4.4.2 Advanced Search Settings 284

4.5 Address Book 285

4.5.1 Creating a Host Account 285

4.5.2 Creating a Group 286

4.5.3 Creating a Folder Link 287

4.5.4 Connecting from Address Book 288

4.5.5 Importing and Exporting the Address Book 289

4.6 Remote ViewLog Service 290

4.6.1 Retrieving Recordings from a Single Host 290

4.6.2 Retrieving Recordings from Multiple Hosts 291

4.6.3 Retrieving Images of Object Index 292

4.6.4 Resuming Backup 293

4.7 Single Player 294
4.7.1 Single Player Window 294
4.8 GPS Tracks Playback 296
4.9 Touch Screen Support..... 298
4.10 Fast Key Reference 299
4.11 Specifications..... 299

CHAPTER

4

Video Playback

Recorded files can be played back using different software applications offered by the system – ViewLog, Quick Search, Remote Playback System and Remote Playback System WebCam version. Following is a comparison table for these applications. This is not a complete comparison table, because many of these features are discussed in details throughout the manual. However, this table may help you to decide which application to use under a given situation.

Application	Description
ViewLog	A full-function player, allowing you to play back video, search a video event, merge and export video and etc. See *4.1 Playing Back on ViewLog*.
Object Search	A more convenient tool that allows you to search video files recorded on motion or alarm. See *4.2 Object Search*.
Quick Search	Searches and plays back POS events. See *4.4 Quick Search*.
Remote Playback Server WebCam version	No additional software installation is necessary. Just play back using your Web browser. See *Remote Viewing* in Chapter 8.
Single Player	Plays back the backup recorded files. Provides simple and easy playback functions. See *4.8 Single Player*.

4.1 Playing Back on ViewLog

The ViewLog plays back recorded video files without affecting recording. There are two ways to launch ViewLog:

⌘ Start **VideoLog** from the folder (Windows Start menu/Programs)

⌘ On the Main System, click the **ViewLog** button (No.13, Figure 1-2) and then select **Video/Audio Log**. Or press **[F10]** on the keyboard.

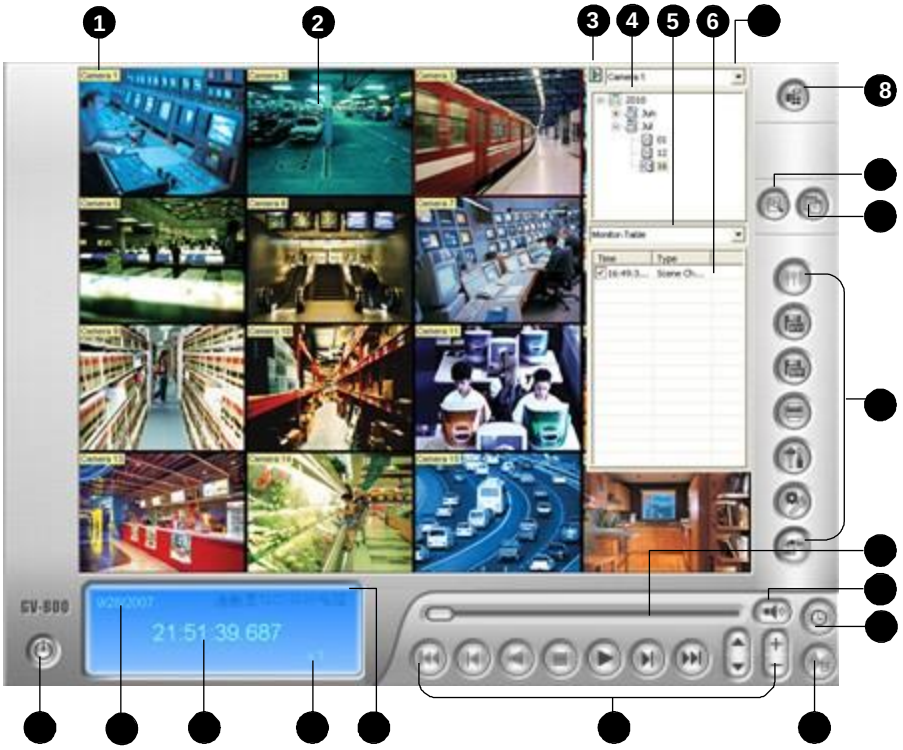


Figure 4-1 *The ViewLog Window*

Without further settings you can play back the event by clicking the **Play** button on Playback Panel. Click the **View Mode** button (No. 8, Figure 4-1) to switch the current view mode to a multi-channel view. Use controls on Playback Panel to view the event in the way you want. Move the slider in Playback Meter (No. 12, Figure 4-1) forward and backward to navigate video frames.

To play back multiple events, keep pressing **[CTRL]** on the keyboard and highlight the desired events on the Video Event List (No. 6, Figure 4-1). Then click the **Play** button to play these events. To select events from different dates, click the date from the Date Tree (No. 4, Figure 4-1). Events of that date will be listed in the Video Event List.

The controls in the ViewLog window:

No.	Name	Description
1	Camera Name	Indicates the given camera name.
2	Camera View	Displays the playback video.
3	Arrow Switch	Switches between List Mode and Line Mode. Sets up MDB filter.
4	Date Tree	Displays date folders.
5	Display Option	Specifies the event type to display in List Mode or Line Mode.
6	Video Event List	Displays video events within a certain date folder.
7	Camera Select	Sets a desired camera for display.
8	View Mode	Sets screen divisions: Single View, Panorama View, Quad View or Multi View. Single View also includes these options: Standard, Thumbnail, Mega Pixel (PIP), Mega Pixel (PAP), Geo Fisheye and IMV1 Panomorph.
9	Advanced	Accesses basic search, advanced search and bookmark. Reloads video event list.
10	Normal	Displays or closes the Timeline or Video Event List.
11	Function Panel	Provides various settings for ViewLog.
12	Slider	Moves the slider to rewind or forward the video during playback.
13	Audio Playback	Enables audio playback.
14	Playback Panel	Contains typical playback control buttons.
15	Function Icons	A highlighted icon indicates an enabled function. From left to right are the wide angle lens dewarping, defogging function, stabilizer function, reconnection to Remote ViewLog, A to B Mode, auto playing of next events, the contrast and brightness function, the light enhancement and equalization function, the sharpness and smoothness function and the grayscale function.
16	Playback Speed	Indicates the playback speed x1 represents normal playback speed.
17	Time Display	Indicates the time of the playback video.
18	Date Display	Indicates the date of the playback video.
19	Exit	Closes or minimizes the ViewLog window.
20	A to B Mode	Plays repeatedly the set frames A to B.
21	Playback Mode	Plays back video frame by frame, on real time, with smooth playback or with just key frames.

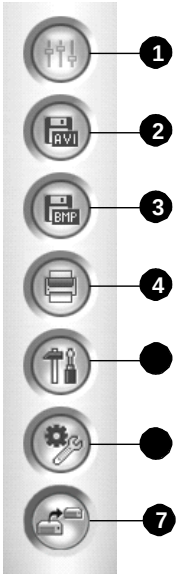


Figure 4-2 *Function Panel*

The controls in the Function Panel:

No.	Name	Description
1	Effects	Adds effects to the images. The effect options include: Contrast/Brightness, Light Enhancement, Equalization, Sharpen, Smooth, Grayscale, Undo to Prev. Action, Undo All Effects, Copy Image to Clipboard, Sample, and Advanced Video Analysis (Defog, Stabilizer, Wide Angle Lens Dewarping). See *Adjusting Distorted Views* later in this chapter.
2	Save As AVI	Save a video file as avi or exe format. See *Merging and Exporting Video* later in this chapter.
3	Save As Image	Save a video image as bmp, jpg, gif, png, or tif format. See *Saving Images* later in this chapter.
4	Print	Specifies various settings for printing.
5	Setting	Accesses system settings of ViewLog. See *Advanced Settings* later in this chapter.
6	Tools	Brings up these options: Object Search, Advanced Log Browser, Delete Log, Remote ViewLog Service, Remote Storage System, Address Book, Display GIS Window, Select Map API, and Tool Kit. See *Object Search, Advanced Log Browser, Remote ViewLog Service* later in this chapter.
7	Backup	Backs up video files. See *Chapter 5 Backup, Deletion and Repair*.

4.1.1 Playback Screen Layout

Click the **View Mode** button (No. 8, Figure 4-1) any time when you want to change the current view mode.

④ **Single View:** Includes the following types of layouts:

Standard: Displays one playback channel only.

Thumbnail: Reviews images frame by frame in thumbnails,.

Mega Pixel (PIP): Crops a video to get a close-up view or zoom in on the video. For details, see *Picture-in-Picture View* in Chapter 1.

Mega Pixel (PAP): Creates a split video effect with multiple close-up views on the image. For details, see *Picture-and-Picture View* in Chapter 1.

Geo Fisheye: Displays the fisheye images recorded with -Fisheye Camera or third-party fisheye cameras in different view modes. For details, see *Fisheye View* in Chapter 3.

IMV1 Panomorph: Displays the fisheye images recorded with an ImmerVision IMV1 Panorama Lens in different view modes. For details see .Step 1 in *Setting Up a -Fisheye Camera* earlier in this chapter.

④ **Panorama View:** Plays back in continuous scenes. For details, see *Panorama View* in Chapter 3.

④ **Quad View:** Plays back in a quad layout. For details, see *[Quad View]* in *Advanced Settings* later in this chapter.

④ **Multi View:** Plays back up to 16 camera recordings. For details, see *[Multi View]* in *Advanced Settings* later in this chapter.

The option of Thumbnail View is disabled while a video file is playing back. Wait until the video ends or click the **Pause** button to make the option available.

In a thumbnail view, a video file is divided into a set of frames. The frames are displayed in 25 playback windows, shown as follows. This helps to locate required frames you may otherwise miss by other viewing methods.

Figure 4-3

4.1.2 Playback Control Buttons

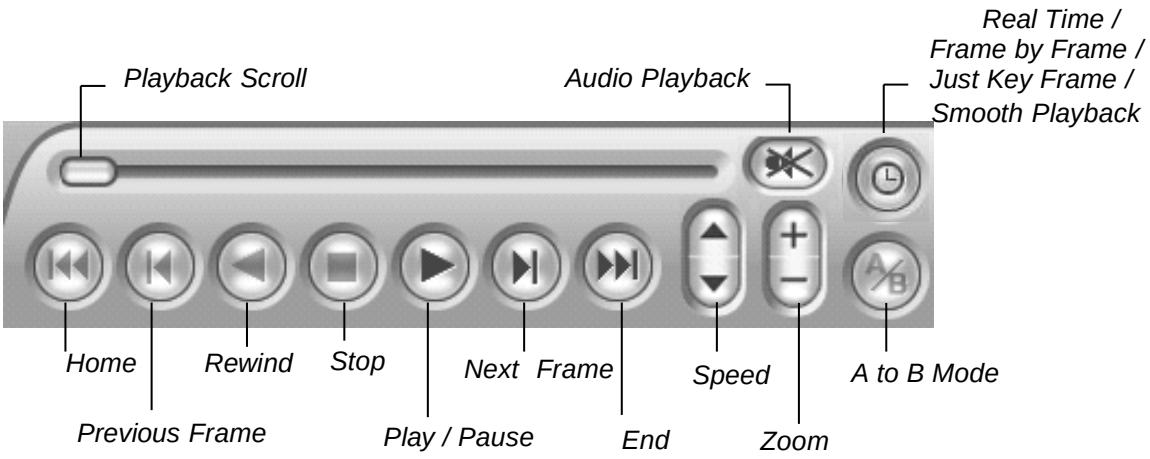


Figure 4-4

Playback Mode Option

By default, the ViewLog is set to play back video in real time mode. To change playback modes, find the button on the Playback Control Panel.

④ **Frame by Frame (without audio):** Plays back video frame by frame without audio. This method delays playback depending on bandwidth and computer performance, but all video frames are fully played back. When the view mode is set to be Panorama View, Quad View or Multi View, this is the default play mode.

④ **Real Time:** Plays back video on real time. This method saves waiting time for rendering, but drop frames to give the appearance of real-time playback. When the view mode is set to be Single, the default play mode is Real Time.

④ **Just Key Frame:** Plays back the most representative frames of video. When your network bandwidth is limited, select this option to enhance the playback smoothness.

④ **Smooth Playback:** When the playback appears choppy, select this option to enhance the smoothness.

Note:

1. For the MJPEG codec, every frame is key frame.
2. The Key Frame function only works on V8.3.3 or later. If the version of connected -System, through Remote ViewLog, is earlier than V8.3.3, the Key Frame function is not available.

Zoom Function

When you zoom in, the video will be automatically switched to Picture-in-Picture (PIP) mode if the video resolution exceeds the ViewLog panel. For recordings higher than D1 resolution, you can zoom up to 32 times the original image size; for recordings lower than D1 resolution, you can zoom up to 8 times the original image size.

A to B Playback Mode

When playing video events, you can set a starting and an ending frame for auto-playing:

1. To set the starting frame A, click the **A to B Mode** button (Figure 4-4). The message *A to B Mode (Set A)* appears on the screen.
2. To set the ending frame B, click the **A to B Mode** button. The message *A to B Mode (Set B)* appears on the screen.

ViewLog will start playing the set frames A to B repeatedly. To stop the playing, click the **A to B Mode** button; the message *A to B Mode (Cancelled)* will appear.

4.1.3 Recycling Option for Video Files

You can choose whether to recycle your video files. To apply this function, follow the steps below.

1. Select a desired video event from Video Event List (No. 6, Figure 4-1), and then right-click it to call up a menu as shown below.

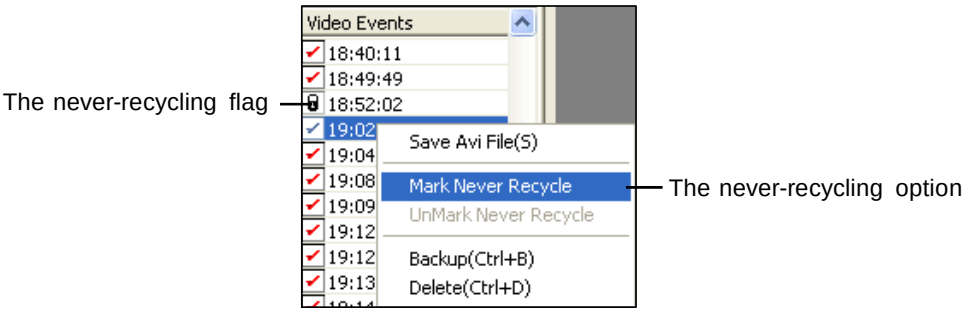


Figure 4-6

2. Select the **Mark Never Recycle** option. A never-recycling flag will appear next to the video event.
3. To disable the never-recycling function, right-click the video event again and select **Unmark Never Recycle**.

Unmarking All Never-Recycling Flags

The above step 3 illustrates how to unmark never-recycling flag one by one. When you like to unmark all the never-recycling flags in certain cameras, follow the steps below.

1. Shut down ViewLog and Main System if they are running.
2. Go to the Windows **Start** menu, select **Programs**, point to the folder, and then click **RepairLog500.exe**. A valid ID and a password are required.
3. When the Select Camera for Repair Database dialog box appears, select the cameras of video files that you want to unmark their never-recycling flags.
4. Click **OK** to open the Repair Database dialog box. See Figure 5-8 in Chapter 5.
5. Clear the selection of **Reserve Never-recycle Flag**.
6. Click the **Use Default Path** button to unmark all the never-recycling flags.

Reserving Never-Recycling Flags

If you like to reserve all the never-recycling flags you marked on video events even after repairing the database, select **Reserve Never-recycle Flag** on the Repair Database window before making repairs. See Figure 5-8 in Chapter 5.

4.1.4 Bookmarking a Frame

You can create a bookmark for a video frame and later return to that frame quickly or resume a video from where you bookmarked.

Creating a Bookmark

1. Click the **Pause** button at the frame you want to bookmark.
2. Right-click the frame and select **Add to Bookmark**. The Bookmark Description dialog box appears.

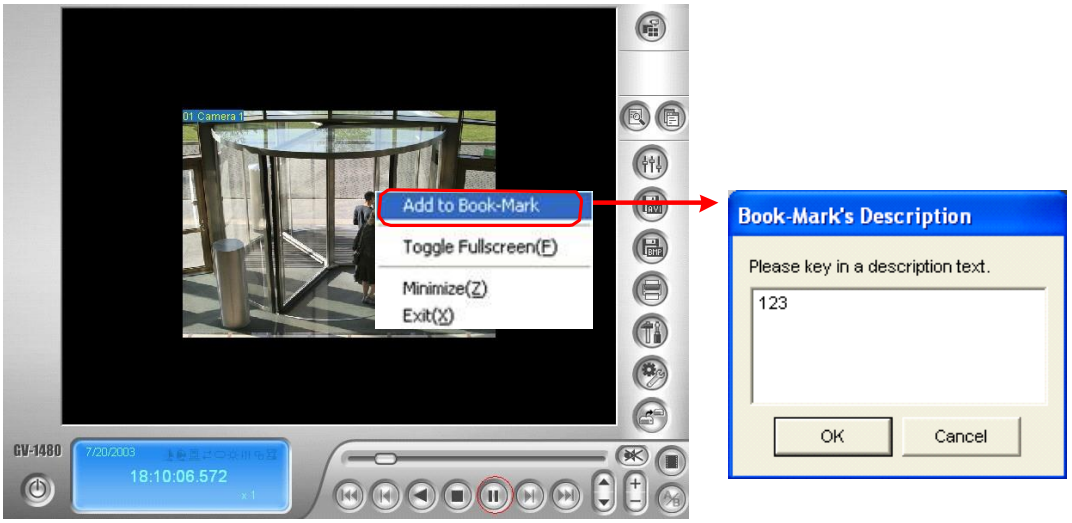


Figure 4-7

3. Type the text for the bookmark label.

Note: By default, bookmarked frames are saved at :\ xxx\Bookmark and are in JPEG format.

Viewing a Bookmark

1. Click the **Advanced** button (No. 9, Figure 4-1) and select **Bookmark**. The Bookmark window appears.

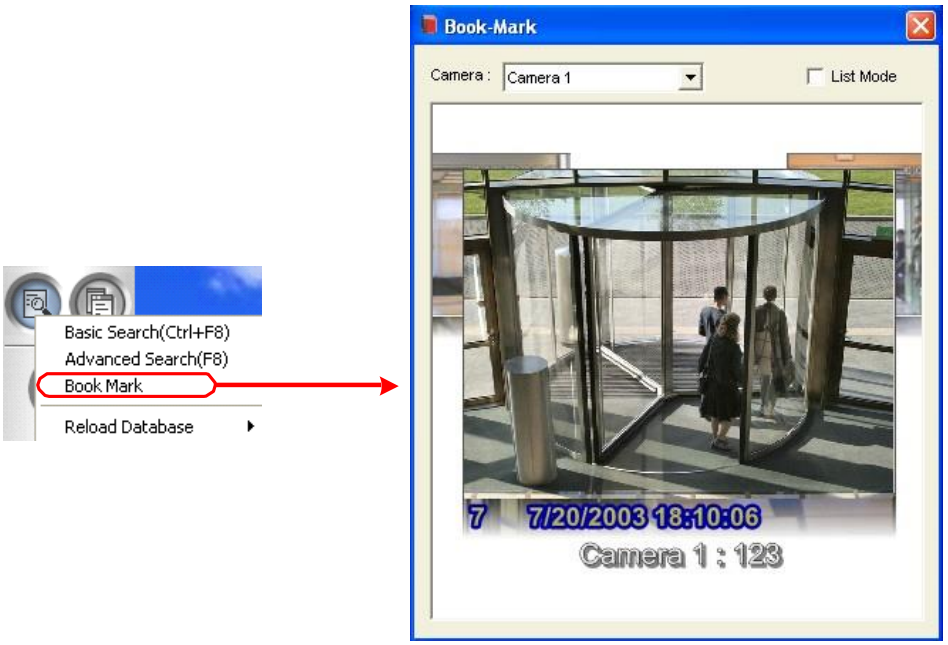


Figure 4-8

2. In the Camera drop-down list, select a desired camera to display its bookmarks, or select **All** to display all the bookmarks.
3. To change a bookmark displayed at the front, click the desired bookmark behind the one at the front. You can also select **List Mode** to display all bookmarks in the thumbnail view.
4. To resume playback from a bookmark, double-click the bookmark. The bookmarked frame is displayed on the ViewLog window. Click the **Play** button to play the video for up to 5 minutes.
5. To rename, delete or import the bookmark, right-click the desired bookmarked frame to have these options.

4.1.5 Searching a Video Event

ViewLog offers four search methods: Basic Search, Advanced Search, List Mode and Line Mode. The four methods allow you to locate a video event recorded by a specific camera and during a specific time period.

Basic Search

1. Click the **Advanced** button (No. 9, Figure 4-1) and select **Basic Search**. This dialog box appears. Alternatively, press **[CTRL]** + **[F8]** on the keyboard to call it up.

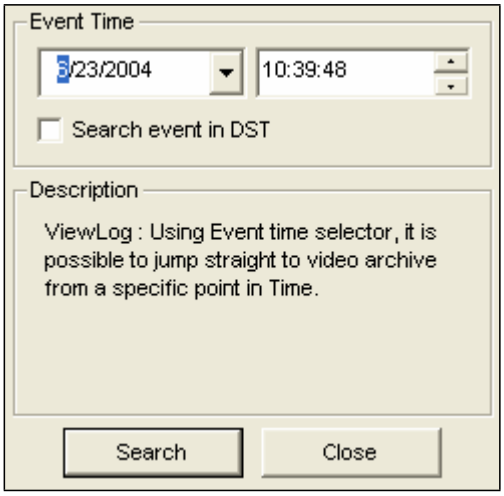

Event Time
3/23/2004
10:39:48
Search event in DST
Description
ViewLog : Using Event time selector, it is possible to jump straight to video archive from a specific point in Time.
Search
Close

Figure 4-9

2. If you want to search the video events recorded during the Daylight Saving Time period, select **Search event in DST**.
3. Specify a desired date and time.
4. Click the **Search** button for the search. If the specified time can't be found, a prompt will appear for you to select a next or previous video event available.

Advanced Search

1. Click the **Advanced** button (No. 9, Figure 4-1) and select **Advanced Search**. This dialog box appears. Alternatively, press **[F8]** on the keyboard to call it up.

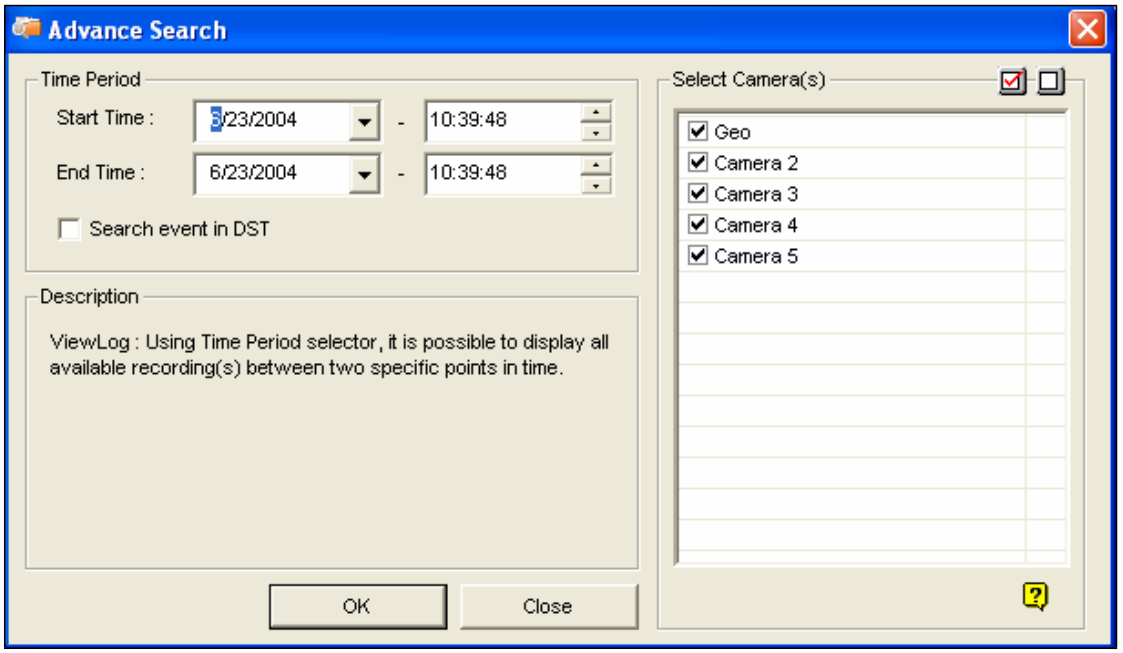


Figure 4-10

2. If you want to search the video events recorded during the Daylight Saving Time period, select **Search event in DST**.
3. Specify the desired date, time period, and cameras for search.
4. Click **OK** to start searching.
5. In the Video Event list, the events matching the search criteria will be highlighted in gray color. Click the **Play** button to play back the highlighted events.

List Mode and Line Mode

The List Mode and Line Mode allow you to see video events listed by date and to search events by event types or a POS item. The List Mode displays events in an Event List, while the Line Mode displays events in a timeline. To switch between the two modes:

1. Click the **Normal** button. The List Mode or the Line Mode window appears.
2. Click the arrow on the top left corner.

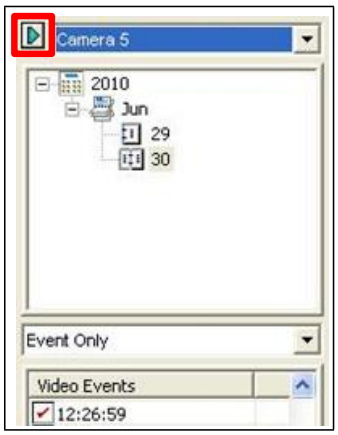


Figure 4-11

3. Select **Switch Time Mode**, and select **List Mode** to see the Video Event List or **Line Mode** to see the Event Timeline.

List Mode

1. Select a camera from the drop-down list.
2. Click the date tree to see video events recorded on that day.
3. To choose what information to display in the Video Event List or to search by event types or a POS item, select one of the following display options from the drop-down list.

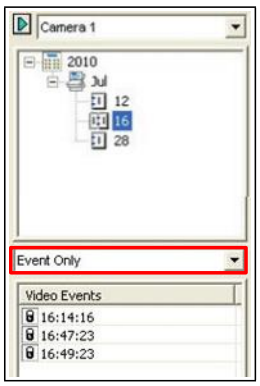


Figure 4-12

- **Event Only:** Lists the video events only.
- **Event + Total Frame:** Lists the video events and their total number of frames.
- **Event + Total Time:** Lists the video events and their total time length.
- **Event + Total Size:** Lists the video events and their total file size.
- **Never-Recycle Events:** Lists the never recycle video events only.
- **Monitor Table:** Lists the types of video events selected in MDB filter. See the section below on how to set up the MDB filter.
- **POS Table:** Lists the video events with the item specified in MDB filter for each POS device. See the section below on how to set up the MDB filter.

Line Mode

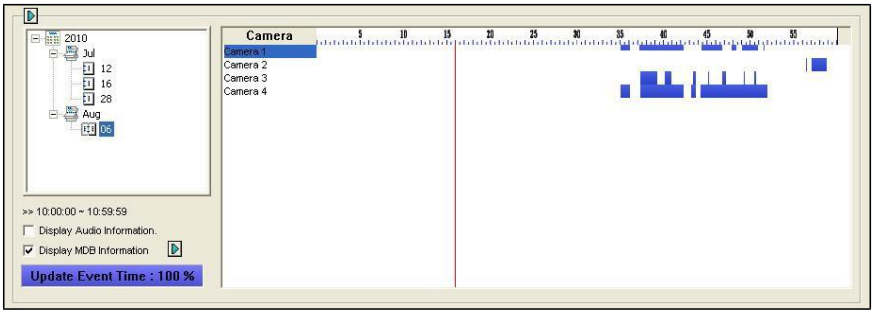


Figure 4-13

1. To see video events on a particular day, click the date tree.
2. Move the mouse pointer on the desired blue block of that camera, and right-click it to have the sub Timelines of hour mode and minute mode. Three types of timeline modes are available:
   - ④ **Change to day mode:** The default mode displaying at which hour the events have been recorded.
   - ④ **Change to hour mode:** Opens the sub Timeline displaying at which minute the events have been recorded.
   - ④ **Change to minute mode:** Opens the sub Timeline displaying at which second the events have been recorded.
3. To display the audio information for each camera on the timeline, select **Display Audio Information**.

4. To search events by event types or a POS item, select **Display MDB Information** and click the Arrow button. Select **Monitor Table** to see the events types selected in the MDB filter and select **POS Table** to see the POS item specified in the MDB filter. The selected event types or POS item are marked in orange. See the section below on how to set up the MDB filter.

Setting up the MDB filter:

1. Click the arrow on the top-left corner of the event search window.
2. Select **MDB Filter**. This dialog box appears.

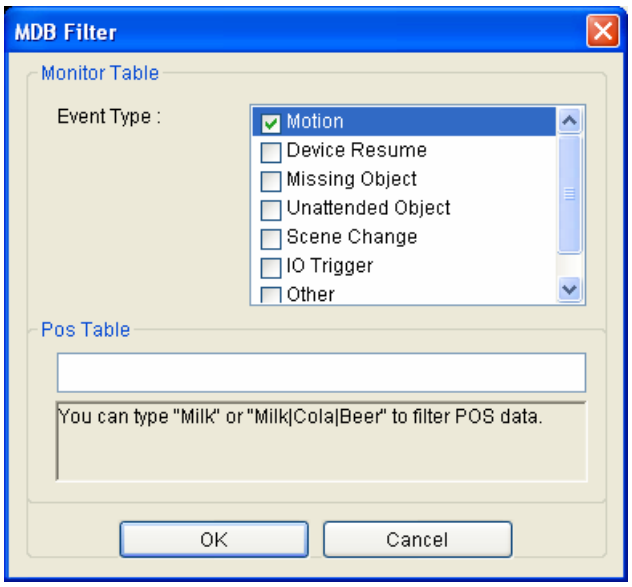


Figure 4-14

3. Select the types of events or type the POS item you want to search.
4. Click **OK**.

Note: The MDB filter only sorts out the events recorded in the System Log. To record motion detection events in the System Log, ensure to select **Register Motion Event** (Configure button < System Configure < Camera Configure).

4.1.6 Merging and Exporting Video

You can merge several video files into a single file and export it in AVI format. You can also choose to export the file in EXE format which allows you to play video with any multimedia player.

Simple Merge

Simple Merge allows you to merge several video files into a single file.

Note: The maximum size of the merged file is 2 GB. If the merged file is over the limit, it will be split up into another file.

---

1. From the Video Event list (No. 6, Figure 4-1), select one event or several events by using **Ctrl + left click**.
2. Select the screen division from the View Mode button (No. 8, Figure 4-1).
3. Click the **Save As AVI** button (No. 2, Figure 4-2). This dialog box appears.

   Alternatively, press **[S]** on the keyboard to call it up.

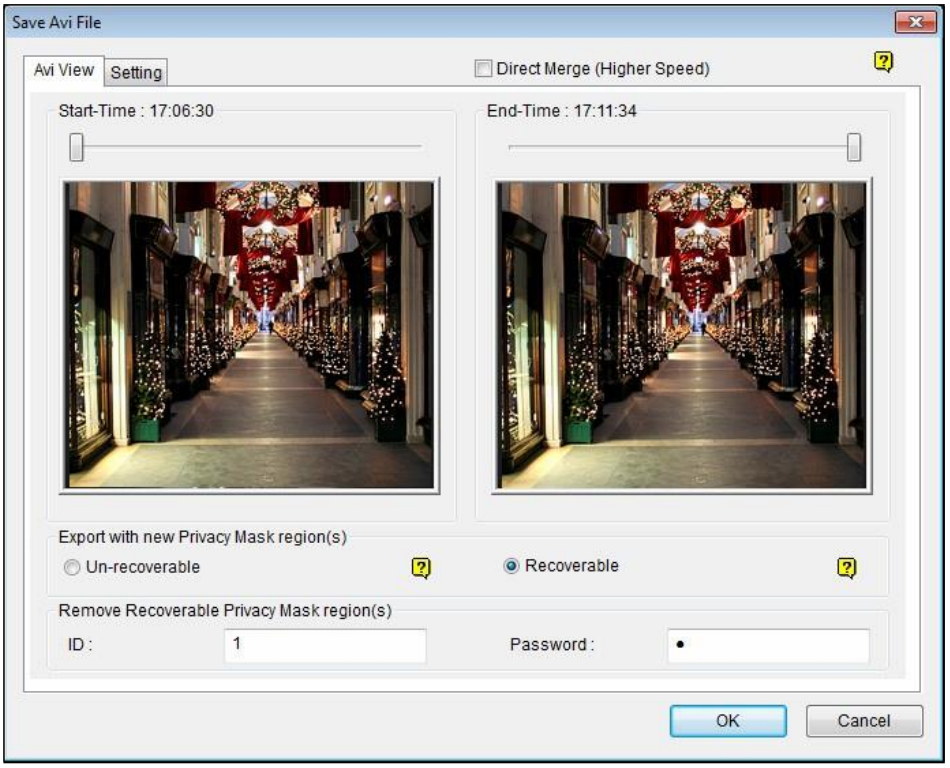


Figure 4-15 *Save AVI File*

4. Drag the timelines to define a starting and ending time of the file.
5. If the video event has the Privacy Mask settings, and you want to retrieve the recoverable block-out area(s) in the exported file, type a valid ID and password in the Remove Recoverable Privacy Mask region(s) field. If you want to remain the recoverable block-out area(s) in the exported file, leave the field blank.
6. If you want to add more Privacy Masks onto the video, follow the instructions in *Privacy Mask Settings* later in this chapter.
7. If you want to save the video file in the codec type that it was originally recorded in, enable **Direct Merge (Higher Speed)**.

Note: Once the **Direct Merge (Higher Speed)** is enabled, you will not be able to customize settings such as codec selection, privacy mask recoverability and digital watermark, but the time required for conversion is significantly reduced.

---

8. To configure the saving path and format of the exported video, click the **Setting** tab. For details see *AVI File Settings* later in this chapter.
9. Click **OK** to export and save the file.

Advanced Merge

Advanced Merge allows you to merge several AVI files into a big single file or into a number of files of a set duration.

1. On the function panel, click the **Save as AVI** button (No. 2, Figure 4-2) and select **Advanced Merge**. This dialog box appears.

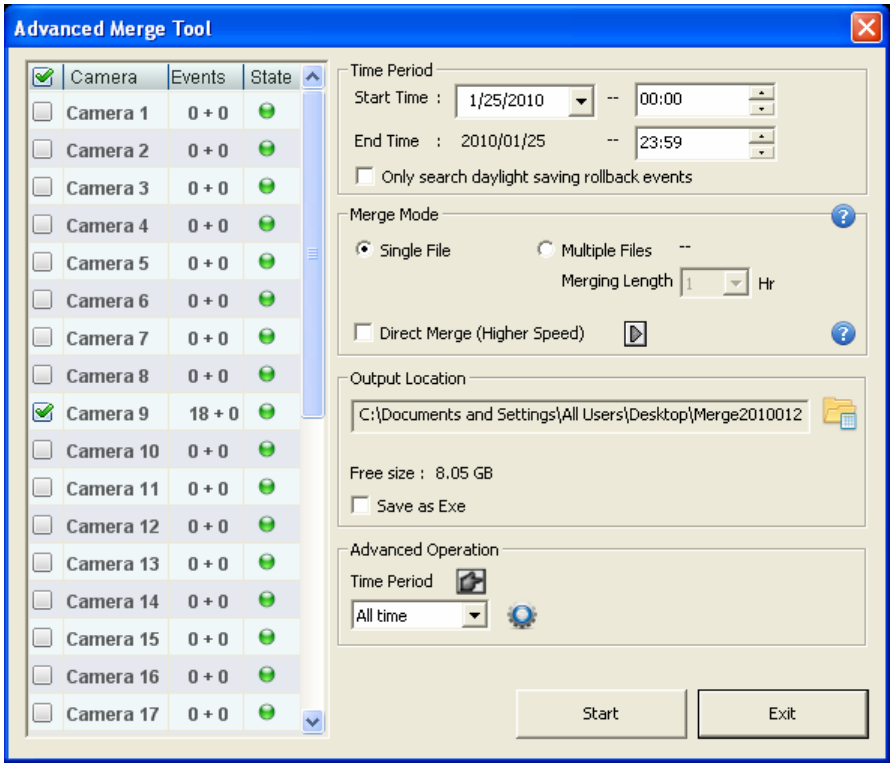


Figure 4-16

2. In the Time Period section, specify Start and End time to locate files. The number of video and audio files for each camera found within the specified time is displayed on the left camera list. For example, “Camera 9 18+0” means the Camera 9 has created 18 video files and 0 audio files within the specified time. By default you can only merge the files of one day.
3. In the Merge Mode section, select one of the merging methods:

   ④ **Single File:** Merges several AVI files into a single file. The maximum size of the merged file is 2 GB for FAT32 and NFTS file systems. If the merged file exceeds the limit of Windows file system, it will be split up into another file.

   ④ **Multiple Files:** Merges AVI files into several files of a specific duration. After specifying the duration, you can see the number of merged files will be created.

   ④ **Direct Merge (Higher Speed):** The merging method only joins video files together without the inclusion of their video effects, such as privacy masks, watermarks, time stamps, GPS data and etc.

- ⌘ Using the Direct Merge to merge several AVI files into a single file, also select **Single File**.
- ⌘ Using the Direct Merge to merge AVI files based on the specified duration, also select **Multiple Files**.
- ⌘ To merge audio and video together, click the arrow button and select **Include Audio**.

Since the exclusion of video effects, the Direct Merge is faster than the other two merging methods.

4. In the **Output Location** section, specify the storage location of merged files, and select whether to save merged files in EXE format.
5. In the **Advanced Operation** section:
   - ⌘ If you select **Single File** at the step 3, click the button to configure video effects to merged files. For details, see *Merging and Exporting Video* earlier in this chapter.
   - ⌘ If you select **Multiple File** at the step 3, you can define different video effects for each time segment. Select a period of time and click the button to define the video effects to the specific time segment.
6. Click **Start** to begin merging files.

Exporting PIP / PAP View

You can apply PIP (Picture-in-Picture) or PAP (Picture-and-Picture) view to a recorded video and then export the video. The video will be played back in PIP or PAP view.

1. Select a recorded video, click the **View Mode** button, select **Single View** and select **Mega Pixel View (PIP)** or **Mega Pixel View (PAP)**.
2. For PIP View, adjust the navigation box to have a close-up view of the selected area. For PAP View, drag up to 7 areas to see the close-up views.
3. Click the **Save as AVI** button and select **Save as AVI**. The PIP or PAP view you have set appears.

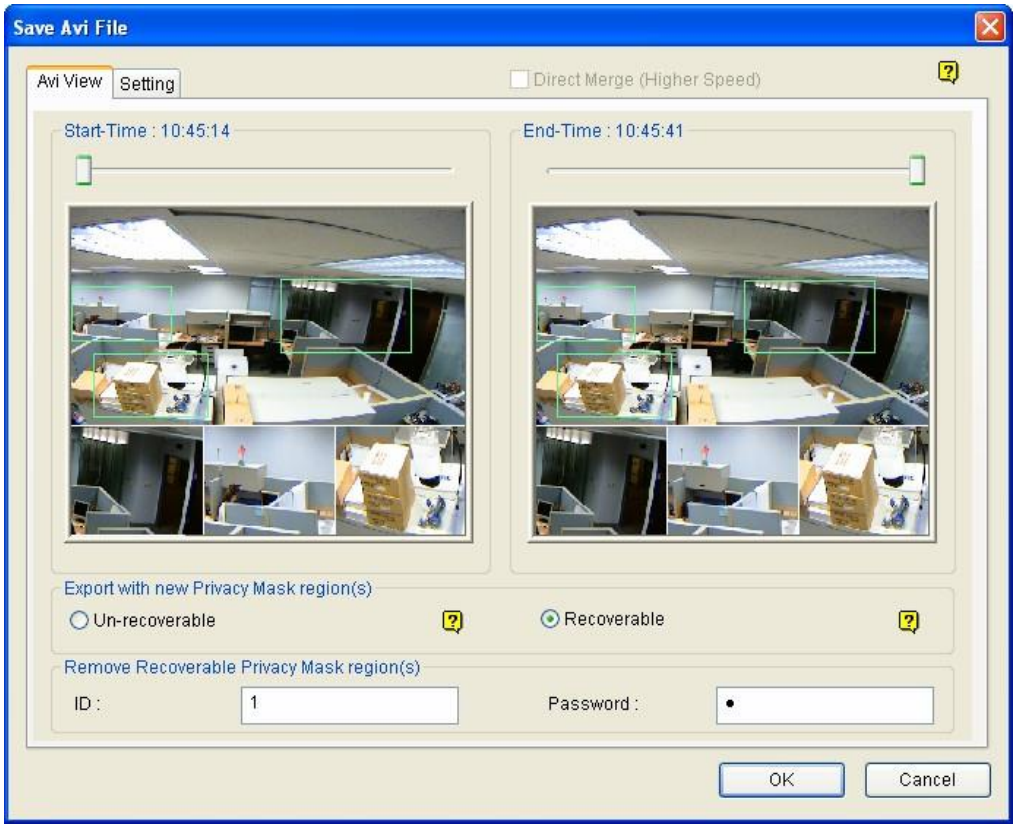


Figure 4-17

4. Click **OK** to export the video. When you play back the video, the PIP or PAP view will be applied.

Note: If the frame of the PIP / PAP navigation box is partially invisible, click the **Setting** tab, click the arrow next to **Video Effects** and clear the selection for **De-Interlace**.

For more details on PIP or PAP view, see *Picture-in-Picture View* or *Picture-and-Picture View* in Chapter 1.

Privacy Mask Settings

In case you forget to set the Privacy Mask at the Main System or need to add more Privacy Masks onto the video for special requirements, you can do that in ViewLog.

1. In the Export with New Privacy Mask Region(s) section (Figure 4-14), select **Un-recoverable** and/or **Recoverable**.
   - ④ **Un-recoverable:** The block-out area(s) in the recorded files cannot be retrieved.
   - ④ **Recoverable:** The block-out area(s) is retrievable with password protection.
2. Drag the area(s) where you want to block out on the image. You will be prompted to click **Add** to save the setting.

Using a valid ID and Password, you can retrieve the recoverable block-out area(s) in the exported file. For details on the Privacy Mask, see *Privacy Mask Protection* in Chapter 3.

AVI File Settings

To configure the format of exported video, follow these steps:

1. Click the **Setting** tab in the Save AVI File dialog box. Note that when you save the AVI file in single view mode, the window looks slightly different.

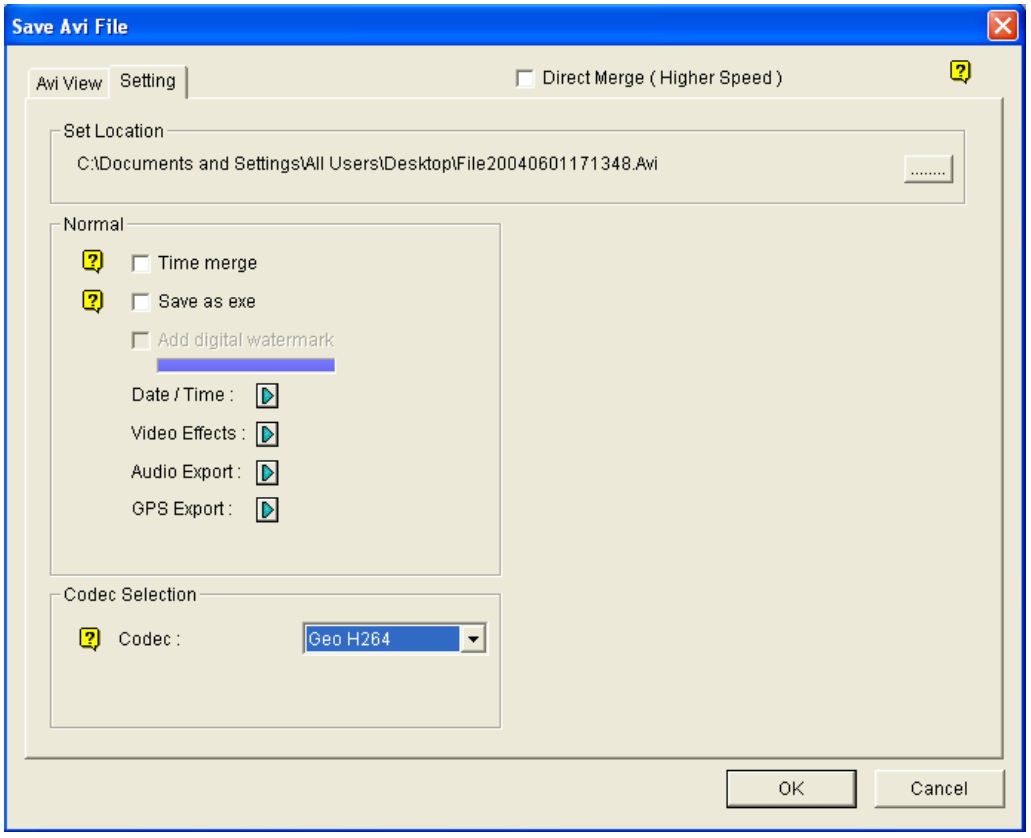


Figure 4-18

[Set Location] Click the **[…]** button to assign a saving path.

[Normal]

- **Time Merge:** Select whether to save a full-length video with recorded and non-recorded periods. The non-recorded period will display a blank blue screen. This option is designed to accurately reflect your recording status.
- **Save as EXE:** Select whether to save files in EXE format. Enable this feature if you want to play back video at the computer without installing -System. This format allows you to auto-play the files with any third-party player.
- **Add digital watermark:** Select whether to include the watermark in the exported video. This option is only available when the watermark has been applied on the recorded video.
- **Date/Time:** Select whether to include date and/or time stamps. You can also select the font type and size, stamp position and color on the images.
- **Video Effects:** Select whether to include the special effects in the exported video. To include the effects of De-Interlace, Defog, Stabilizer, Overlay's Camera and Time and Overlay's POS, you must have applied these functions on the recorded video.
- **Audio Export:** Select **Denoise** to remove audio noises from the video, or select **Channel** for audio exporting.
- **GPS Export:** Select **Channels** to export the GPS data recorded on the -System. .

[Codec Selection]

- **Geo H264:** This codec is created by Sting Alarm. It provides better image quality, higher frame rates and smaller files size than any other. If the codec is selected, you must play the exported files on the computer with the Geo codec installed. Otherwise you can export the files in EXE format in order to play the video at any computer.
- **WMV9:** This code is created by Microsoft. It allows you to play the video with Windows Media Player directly without using Sting Alarm codec. If the codec is selected, the Privacy Mask you created using the ViewLog will be disabled.

2. Click **OK** to apply above settings.

4.1.7 Extracting Frames from a Video Event

You can extract certain frames of a video event and save them as another event.

1. Click the **Save As AVI** button (No. 2, Figure 4-2), and select **Display Merging List**. This dialog box appears.

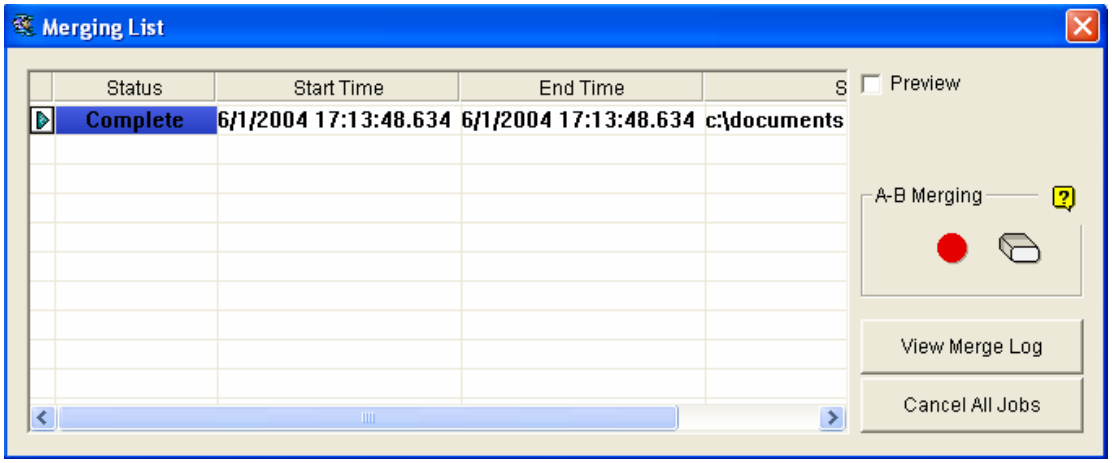


Figure 4-19

2. Select a desired video file from the Video Event list.
3. Click the **Play** button on the Playback Panel to play the video.
4. To set the start frame, click the **A to B Mode** button ● in the Merging List dialog box. The button turns black. If you want to reset the start frame, click the **Cancel** button and then click the **A to B Mode** button ● again to set a new start frame.
5. To set the end frame, click the **A to B Mode** button ●. The system starts extracting the specified frames from the file. When the extract is complete, the Status field displays “Complete”.
6. To view the extract, click the arrow button on the list, and select **Play**.
7. To view where the file is located, click the arrow button on the list and select **Open Path**.

Note: If you want to clear the entries on the Merging List, click the arrow button beside the desired entry, and select **Clear**. The entry will be deleted, but the saved file is still kept in the storage location.

4.1.8 Saving Images

You can save the current camera view as an image file.

1. Click the **Save As Image** button (No. 3, Figure 4-2). This dialog box appears.

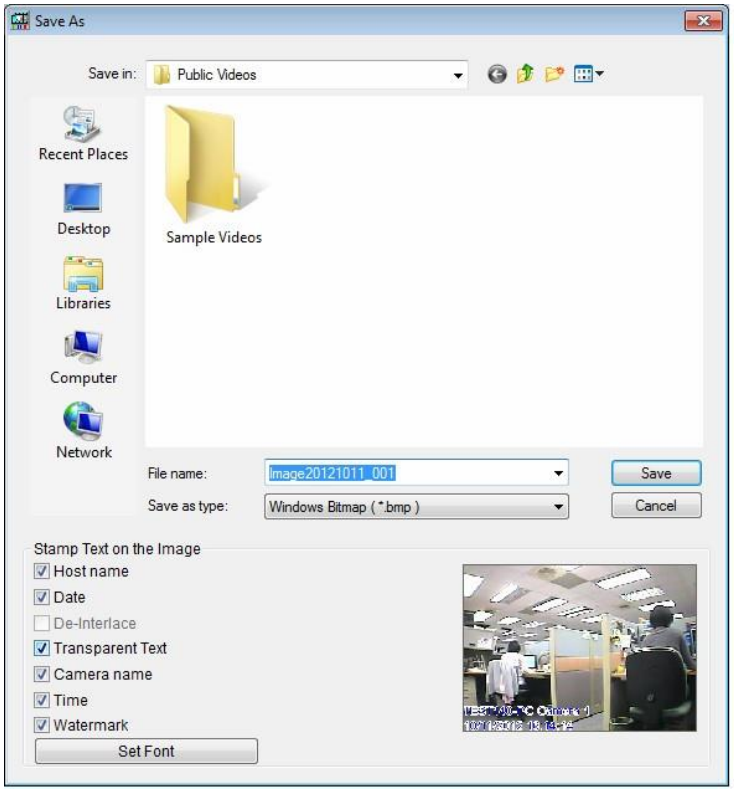


Figure 4-20

[Stamp Text on the Image]

Select whether to include host name, camera name, date and/or time stamp on the image.

Selecting **Transparent Text** will create the stamp on the transparent background.

Selecting **Watermark** and **Deinterlace** will include the two features in the saved image.

[The image] Click on the image at the bottom to preview the stamp text. Click on the image again to close the preview window.

2. Name the file, select a file format, and then assign the location to save the image file.

4.1.9 Printing Images

You can print images in three layout styles: single view, quad view or multi view.

1. Click the **View Mode** button (No. 8, Figure 4-1) to decide the screen layout.
   Note that Thumbnail View is not available for print.
2. Select an event in the Video Events list (No. 6, Figure 4-1), and then click the **Print** button (No. 4, Figure 4-2). This dialog box appears.

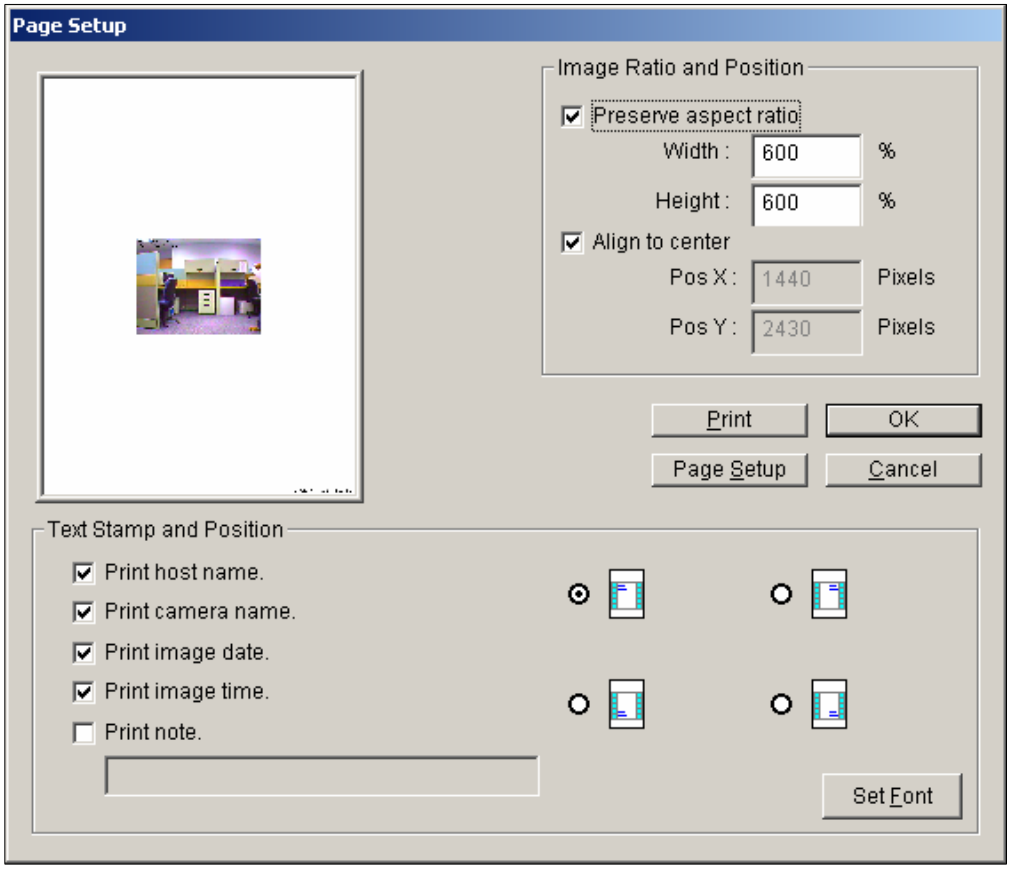


Figure 4-21

[Image Ratio and Position] Changes the size of the image and its position on the page. This option is only available in Single View mode.

④ **Preserve aspect ratio:** Click to maintain the aspect ratio when resizing an image.

④ **Align to center:** Click to change the position of the image on the page.

[Text Stamp and Position]

Select whether to include the host name, camera name, date and/or time stamp on the printed image.

Select **Print note** to include a note below the image. Under the Print note field, type the text of less than 64 characters.

④ **Stamp position icons:** Sets the position where the stamp is printed.

④ **Set Font tab:** Click to select the font type for the stamp.

3. Click **OK** to save the settings or **Print** to print out the page.

4.1.10 Setting Face Mask

You can change the account privileges of Power User, User and Guest to apply Face Mask, which is designed to detect and blur the human faces in recorded videos for privacy purposes. All Supervisor accounts can see the recorded video without face masks.

Figure 4-22

Note:

1. The Face Mask function is designed to detect front-view faces only, and the area of the detected face must take up 10% to 50% of the live image. For other limitations, see *Face Detection* in *Chapter 3*.
2. When the Face Mask function is enabled, the **Speed Up** button will be grayed out.

To Enable the Face Mask for an User Account:

1. On the -System, click the **Configure** button, select **System Configure**, select **Password Setup**, and select **Local Account Edit**. This dialog box appears.

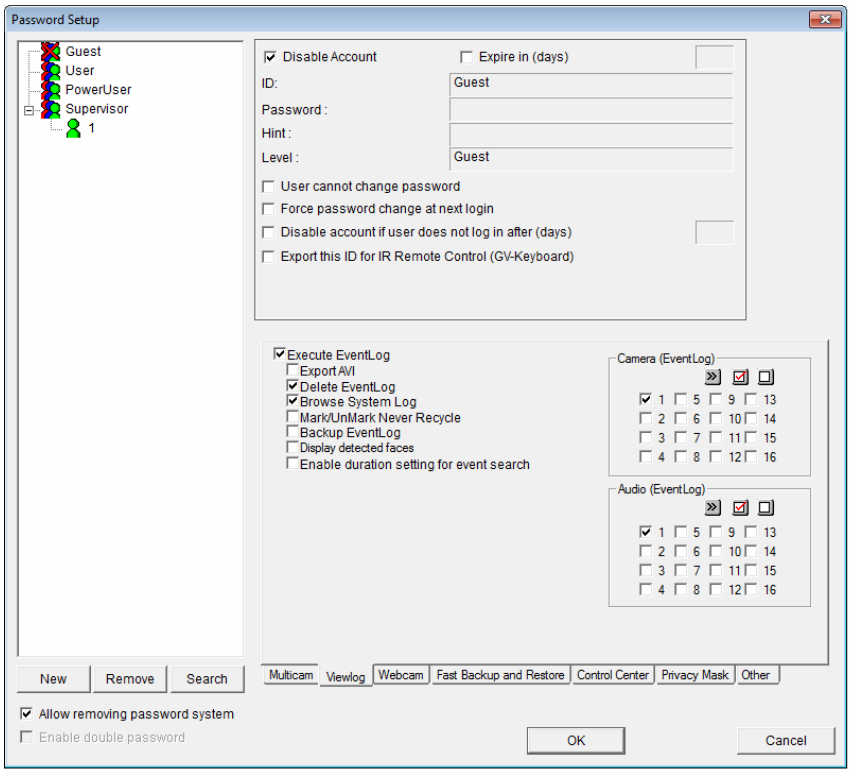


Figure 4–23

2. Select a Power User, User or Guest account and click the **Viewlog** tab at the bottom.
3. Clear the selection for **Display detected faces** to blur human faces when the user watch recorded events in ViewLog.
4. Click **OK**.

4.1.11 Displaying GPS Data

If the recorded video includes GPS data, you can enable GPS data display to see the coordinates and the average speed of the vehicle on the playback video.

1. Click the **Setting** button (No.5, Figure 4-1), click the **Display** tab and select **Display GPS positions**.

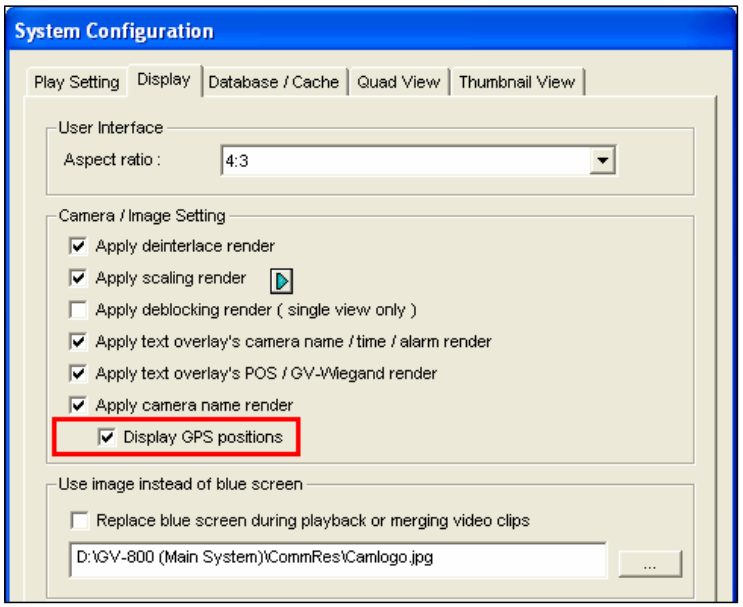


Figure 4-24

2. The coordinates and the average speed of the vehicle will be displayed in the top-left corner on the playback video.

Figure 4-25

4.1.12 Adjusting Distorted Views

When viewing videos through the ViewLog player, images may be curved near the corners. Use the Wide Angle Lens Dewarping feature to correct image distortion.

1. Click the **Effect** button, select **Advanced Video Analysis** and select **Wide Angle Lens Dewarping**. This dialog box appears.

Figure 4-26

2. Select the cameras to apply Wide Angle Lens Dewarping.
3. Click the button to adjust the level of dewarping. This dialog box appears.

Figure 4-27

4. Move the slider at the bottom to adjust the degree of warping. The adjusted view is shown on the right.
5. Click **OK**.

4.1.13 Object Tracking in Fisheye View

You can apply 360° object tracking to video recorded by fisheye cameras.

1. Select a video recorded by a fisheye camera.
2. Click the **View Mode** button, select **Single View**, select **Geo Fisheye** and select **Geo Fisheye: 360 degree**.

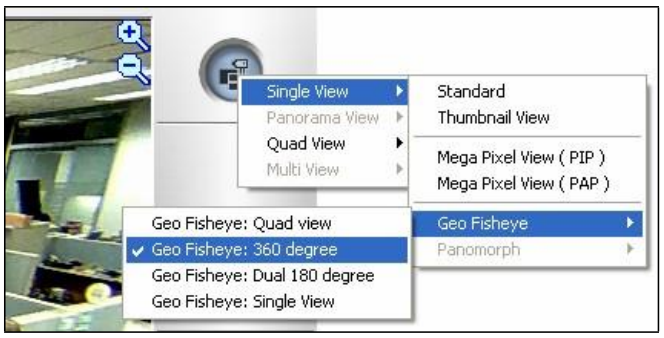


Figure 4-28

3. Right-click the fisheye image, select **Fisheye Option**, select **360 Object Tracking** and select **Advanced Settings**. This dialog box appears.

Figure 4-29

4. Configure the object tracking settings. See *Setting Up a -Fisheye Camera* in Chapter 3.
5. To enable object tracking, right-click the fisheye image, select **Fisheye Option**, select **360 Object Tracking** and select **Tracking**.

6. Click the **Play** button to see object tracking applied to the video.

Figure 4-30

4.1.14 Event Search Limitation

The supervisor can restrict users from accessing all available events and only allow them to view the events of a specified duration in ViewLog. Follow the steps below to prohibit users from changing the event search duration settings.

1. To set the accessible duration of events, click the **Setting** button on the Function Panel (No. 5, Figure 4-2) and click **Database / Cache** tab. For details on duration setting options, see *Database / Cache* in *Advanced Settings* later in this chapter.
2. To prevent users from changing the event duration, on the Main System, click the **Configure** button, select **System Configure**, select **Password Setup**, and select **Local Account Edit**. The Password Setup dialog box appears.
3. Select a Power User or a User account and click the **ViewLog** tab.

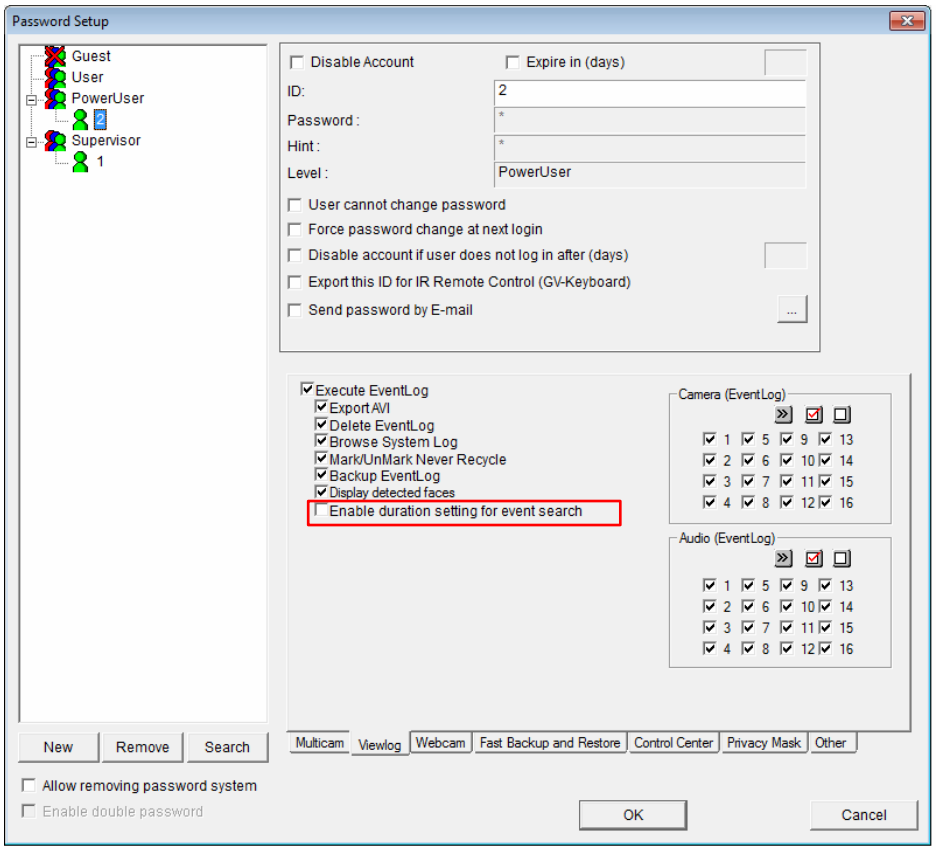


Figure 4-31

4. Clear the selection for **Enable duration setting for event search**. The duration setting options for loading database at ViewLog startup will be grayed out and unchangeable for the selected account.

5. Click **OK** to apply the settings.

Note: The **Enable duration setting for event search** option is selected by default, which allows the duration settings changed by a Power User or User to be applied for all user accounts.

4.1.15 Advanced Settings

The **Setting** button on the Function Panel (No. 5, Figure 4-2) allows you to configure (1) Quad View, (2) Multi View, (3) Thumbnail View, (4) Play Setting, (5) Display and (6) Database / Cache. Click this button to open the System Configuration dialog box.

[Quad View]

You can configure up to 10 sets of Quad Views for simultaneous playback of up to 4 camera recordings. Drag up to four cameras from the right side to the desired number of Quad View.

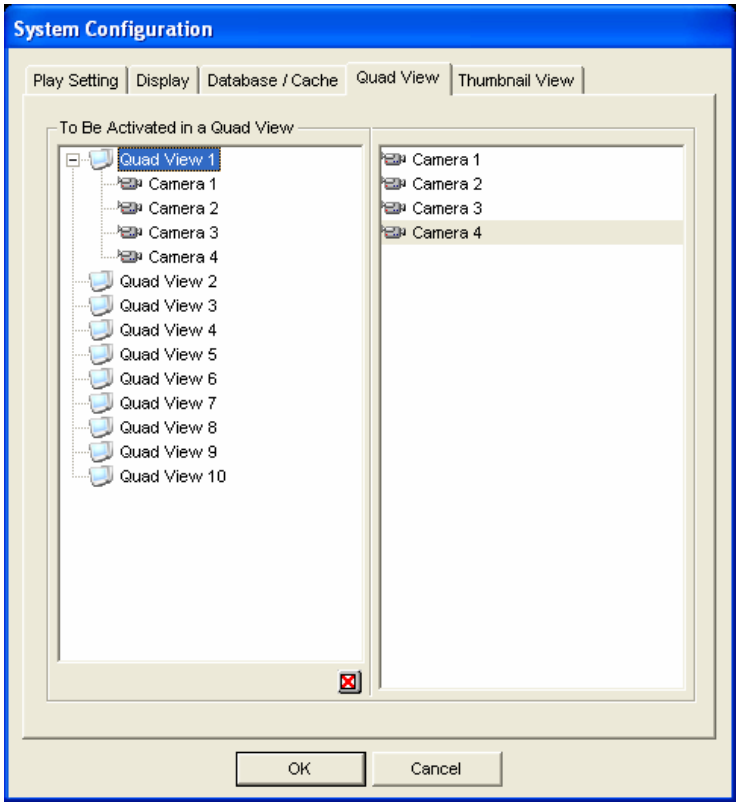


Figure 4-32

[Multi View]

You can configure up to 10 sets of Multi Views for simultaneous playback of multiple camera recordings. In each Multi View you can select the maximum of 16 cameras for playback. Drag up to 16 cameras from the right side to the desired number of Multi View.

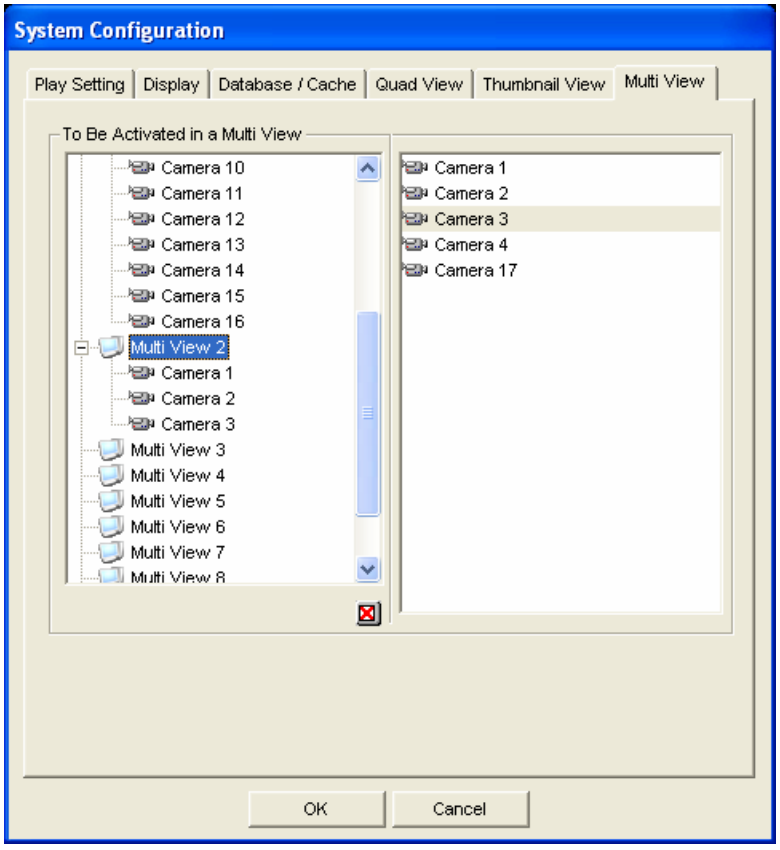


Figure 4-33

[Thumbnail View]

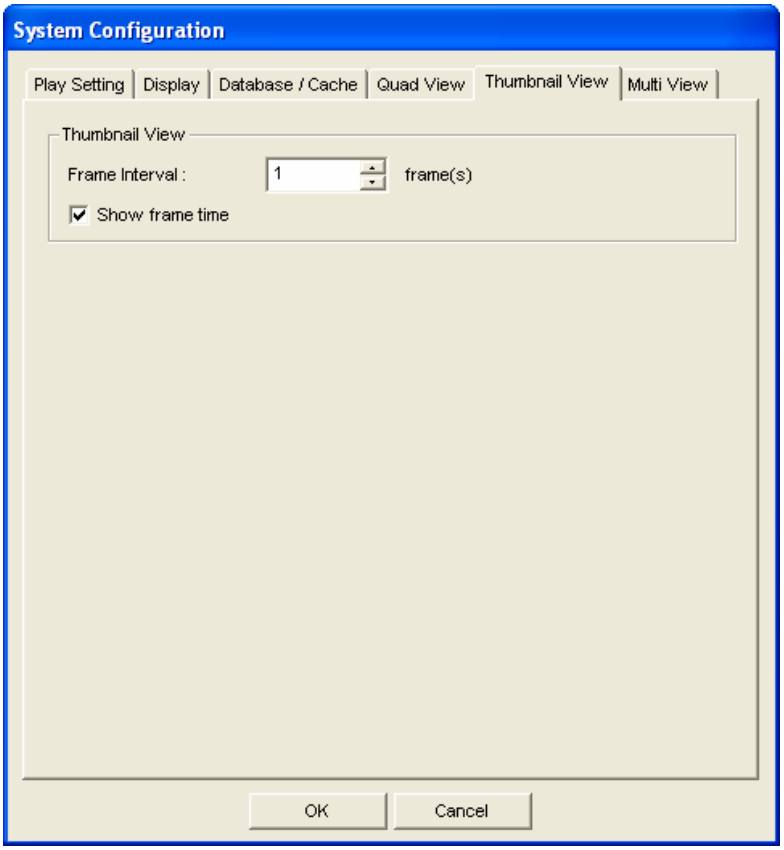


Figure 4-34

④ **Frame Interval:** Specify the number of frames between each video thumbnail. Set the interval between 1 and 600.

④ **Show frame time:** Displays time stamp on each thumbnail.

[Play Setting]

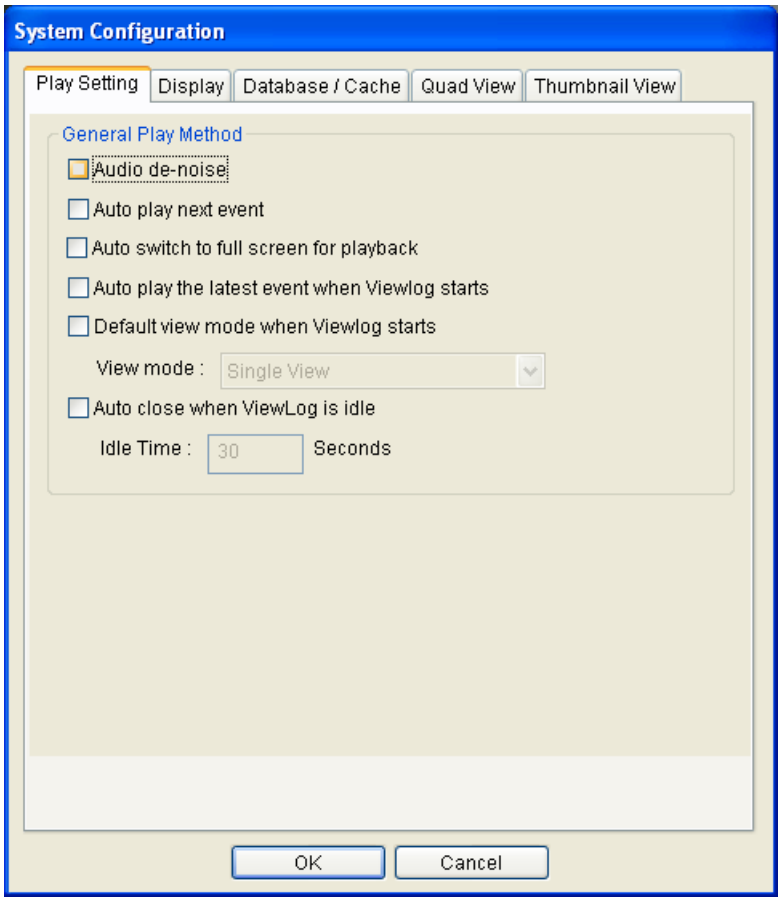


Figure 4-35

[General Play Method]

④ **Audio De-noise:** Improves the audio quality during playback without affecting the files.

④ **Auto play next event:** Puts the next events in sequence for automatic playing.

④ **Auto switch to full screen for playback:** Switches to the full screen when a video is started playing.

④ **Auto Play the latest event when Viewlog starts:** Plays the latest event when ViewLog starts.

④ **Default view mode when Viewlog starts:** Select the desired view mode at startup.

④ **Auto close when ViewLog is idle:** Exits ViewLog automatically after the user remains inactive over the specified timer period. Specify the idle time between 10 to 300 seconds.

[Display]

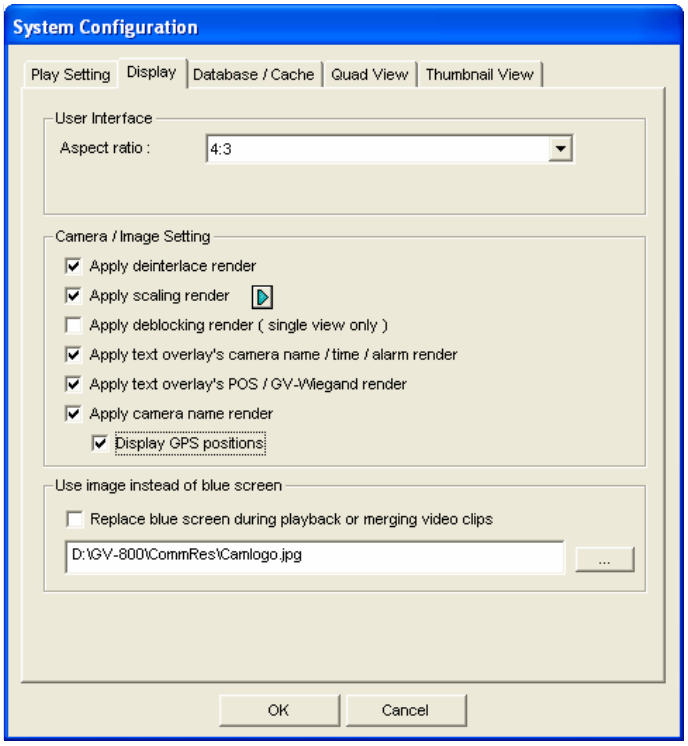


Figure 4-36

[User Interface]

④ **Aspect Ratio:** Select the ratio between the width of the image and the height of the image.

[Camera/Image Setting]

④ **Apply De-interlace Render:** Enable the De-interlace function, and then restart ViewLog to apply it.

Note: This function requires DirectX 9.0C. The De-interlace only works in single view with the resolution of 640 x 480 and 704 x 480.

---

④ **Apply Scaling Render:** Select to smoothen mosaic squares when enlarging a playback video. Restart ViewLog to take effect.

Note: This function requires DirectX 9 and VGA card with the video scaling support. And the scaling only works in single view.

---

④ **Using Colorful Mode:** Click the **Arrow** button beside the Apply Scaling Render option, click the **DirectDraw Scale** tab, and select **Use Colorful Mode**. During playback, you can enhance the coloring to have more vivid and saturated images. Note this function does not affect the original files.

④ **Apply deblocking render (single view only):** Select to remove the block-like artifacts from low-quality and highly compressed video, greatly increasing the overall quality of video.

④ **Apply text overlay's camera name and time render:** Displays the overlaid information of camera ID, location name, date and time on the recorded files. For details, see *POS Data Overlay* in Chapter 7.

④ **Apply text overlay's POS / Wiegand render:** Displays the overlaid information of POS or -Wiegand Capture on the recorded files. For details, see *POS Data Overlay* in Chapter 7.

④ **Apply camera name render:** Displays the camera number and name on the screen.

④ **Display GPS positions:** Displays GPS coordinates on the images when playing the video events recorded with GPS tracks. For details, see *Displaying GPS Data* earlier in this chapter.

[Use image instead of blue screen]

④ **Replace blue screen during playback or merging video clips:** Select a customized image in **.jpeg** or **.bmp** format to replace the blue screen. Note the image size is limited to 704 x 576. The blue screen is the default setting for no image in the recording.

[Database / Cache]

Specify the duration of event files to be loaded at ViewLog startup.

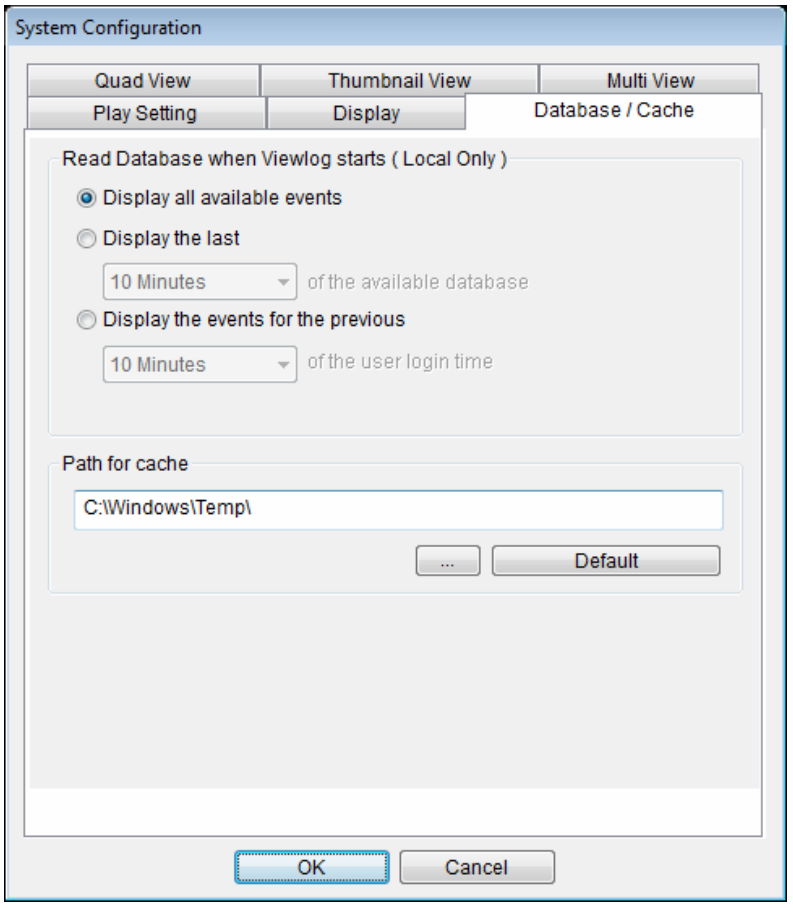


Figure 4-37

④ **Display all available events:** Load all recorded event files.

④ **Display the last [*Time*] of the available database:** Select this option and specify a time period of the last recorded event. For example, if you select **10 Minutes**, user accounts with limited event search privileges will only be able to load the events during the last 10 minutes before the last recorded event file.

④ **Display the events for the previous [*Time*] of the user login time:** Select this option and specify a time period. For example, if you select **10 Minutes**, user accounts with limited event search privileges will only be able to load the events during the last 10 minutes before the account's login time.

Note:

1. If you select the **Display the last or Display the events for the previous** option, the Event List will not be refreshed as the latest event is recorded. To refresh the List, click the **Advanced** button, select **Reload Database**, select **DVR**, and then select

④ **Default Setting** to reload the specified time length of the event files, or

④ **Read All** to reload all record event files.

2. For setting event search privilege for user accounts**,** refer to *Event Search Limitation* in Chapter 4.

[Path for Cache] A cache is memory location that is used to store data temporarily, when you are using the function of Save AVI, Export DVD or Network Buffering. If the default path does not have sufficient space for this temporary storage, assign another path by clicking the **[…]** button.

4.2 Object Search

This feature allows you to perform two functions: 1. Detect motion, missing objects or unattended objects within a certain region of a recorded file. 2. Perform the counting function within certain regions in a recorded file. The following gives an example of motion detection. For details on missing objects, unattended objects and counting, refer to *Object Counting and Intrusion Alarm* and *Unattended and Missing Object Detection* in Chapter 3.

1. Select a desired video file from the Video Event list for the search. Or select multiple files by clicking on each file while keeping pressing **[CTRL]** on the keyboard.
2. Click the **Tools** button (No.6, Figure 4-2) on the function panel, and then select **Object Search** to display the following window.

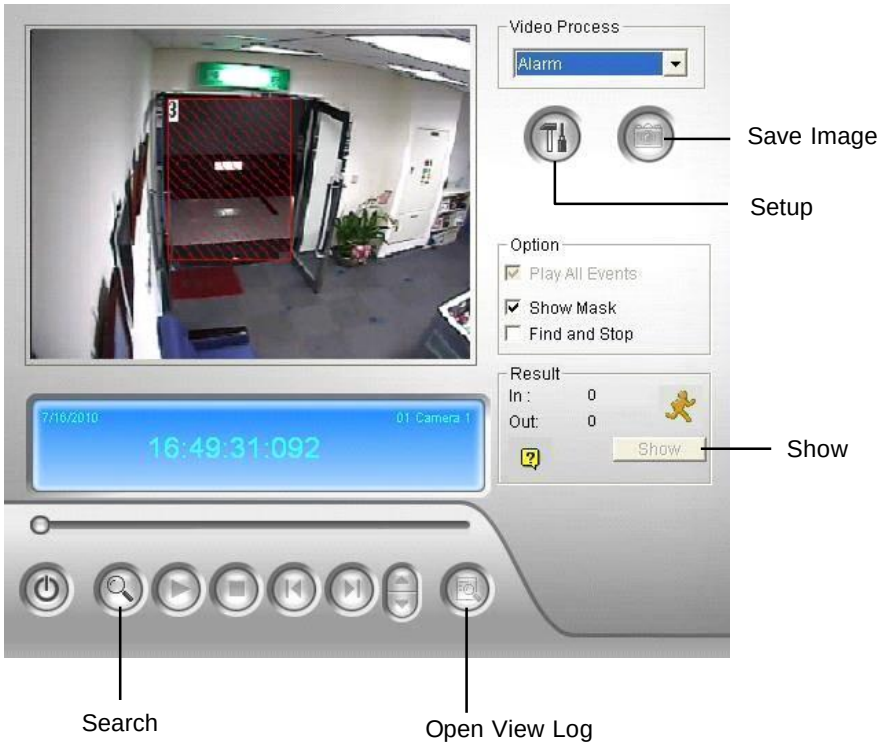


Figure 4-38 *Object Search*

3. In the Video Process drop-down list, select **Alarm**.

4. Click the **Setup** button for further settings. The following window will appear.

Figure 4-39

5. Use the mouse to outline a region for motion detection. You will be prompted to enter **Alarm Region**.
6. Keep detection Sensitivity as defaults or adjust it if needed.
7. Click **OK** to finish the settings and close the window.
8. In the Option section, you have several options:
   - ④ **Play All Events:** Plays back the video segments found as a continuous series of images.
   - ④ **Show Mask:** Shows masks on the detection regions.
   - ④ **Find and Stop:** (recommended) Pauses the search process when motion is detected.
9. In the control panel, click the **Search** button for the search.
10. When any video segment matches the search criteria of motion detection, the **Show** button will be available. Click **Show** to display the Event List window.

Figure 4-40

11. Expand the event folders to see the video segments inside. Or, enable **Show Small Pictures** at the upper of window to access the thumbnail view.
12. Select one video segment, and then click the **Play** button in the Object Search window to play it back. Or, click the **Open Viewlog** button to play it with Viewlog.

4.3 Advanced Log Browser

With the Advanced Log Browser, you can search for log data of monitored events, system activities, user activities, Object Counting events and POS events. For details on the log types, see *System Log* in Chapter 1.

1. Click the **Tools** button (No. 6, Figure 4-2) and select **Advanced Log Browser**. This dialog box appears.

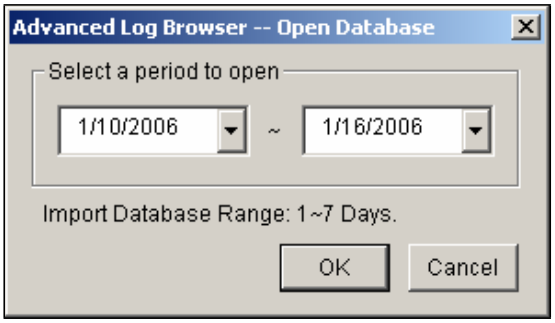


Figure 4-41

2. Specify a time range and click **OK**. All events within the specified range will be displayed on this Advanced Log Browser window.

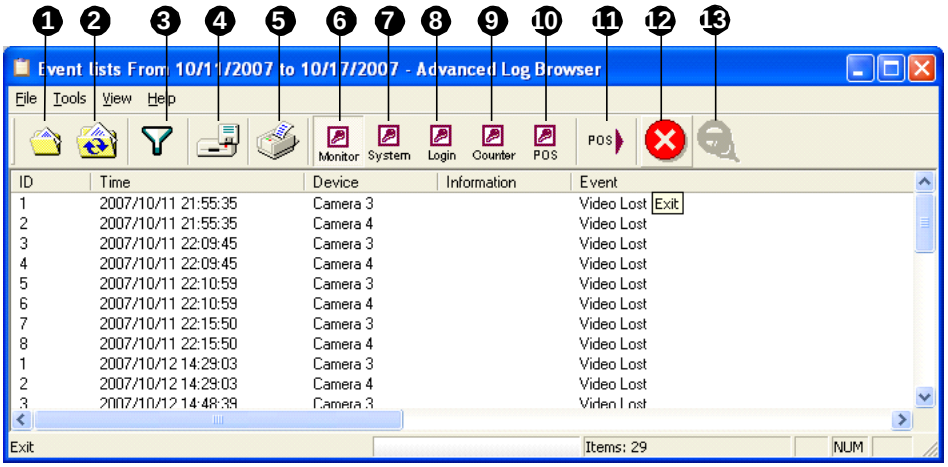


Figure 4-42 *Advanced Log Browser*

The buttons on the Advanced Log Browser:

No.	Name	Description
1	Open	Opens an event log.
2	Reload	Select **Reload All Table** or **Reload Current Table** to refresh loaded data.
3	Filter	Defines the search criteria. See *Filter Settings* later in this chapter.
4	Backup	Select **All Tables** to back up all log data, or selects **Current Table** to back up the current log table you are at.
5	Print	Prints the current log table.
6	Monitor Table	Displays the monitor log.
7	System Table	Displays the system log.
8	Login Table	Displays user's login/logout log.
9	Counter Table	Displays the counter log.
10	POS Table	Displays the POS log.
11	POS List	Accesses one POS channel for log data.
12	Exit	Exits the browser.
13	Filtering / Cancel Filtering	Appears to indicate the filtering process is being performed. You can click it to cancel the filtering. After the filtering is complete, this icon appears dimmed.

4.3.1 Filter Settings

You can define filter criteria to search the desired log data. You can also import pre-defined filter settings for log search, or save current filter settings for future use.

1. On the toolbar, click the desired log table button (Monitor, System, Login, Counter or POS), click the **Filter** button (No. 3, Figure 4-42), and select **Default Filter**. This dialog box appears.

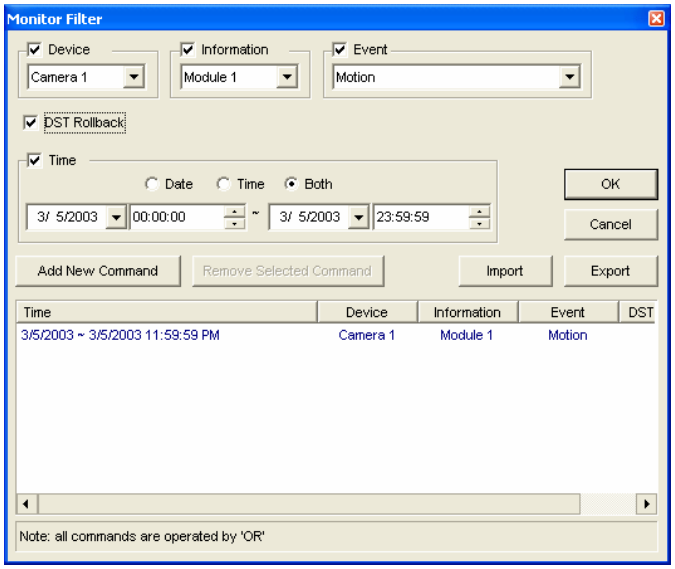


Figure 4-43

2. Define the filter criteria, such as a specific camera and a period of time.
3. If you want to search the log data recorded during the Daylight Saving Time period, select **DST Rollback**.
4. You can click **Export** to save the current settings to another location, or **Import** to apply other filter settings.
5. Click **OK** to display the filter results.

Tip: Next time when you want to use the same exported settings, just click the **Filter** button, select **Favorites**, and select the name of the export file.

Note:

1. The Import and Export features are only available in version 8.1 or later, therefore it is not applicable to export the filter settings to the older version of -System.
2. The default Export path is :\ folder\Syslog_Favorites\Monitor. If you change the saving path, the name of the export file will not be listed in the **Favorites** option.

The POS Filter dialog box has a slightly different look, as illustrated below.

④ **Filter the conditions in below to the selected POS table:** Apply the filter settings to the selected POS devices.

④ **Period between:** Set the employee IDs or names for filtering.

④ **Import / Export:** Import or export the POS Filter settings.

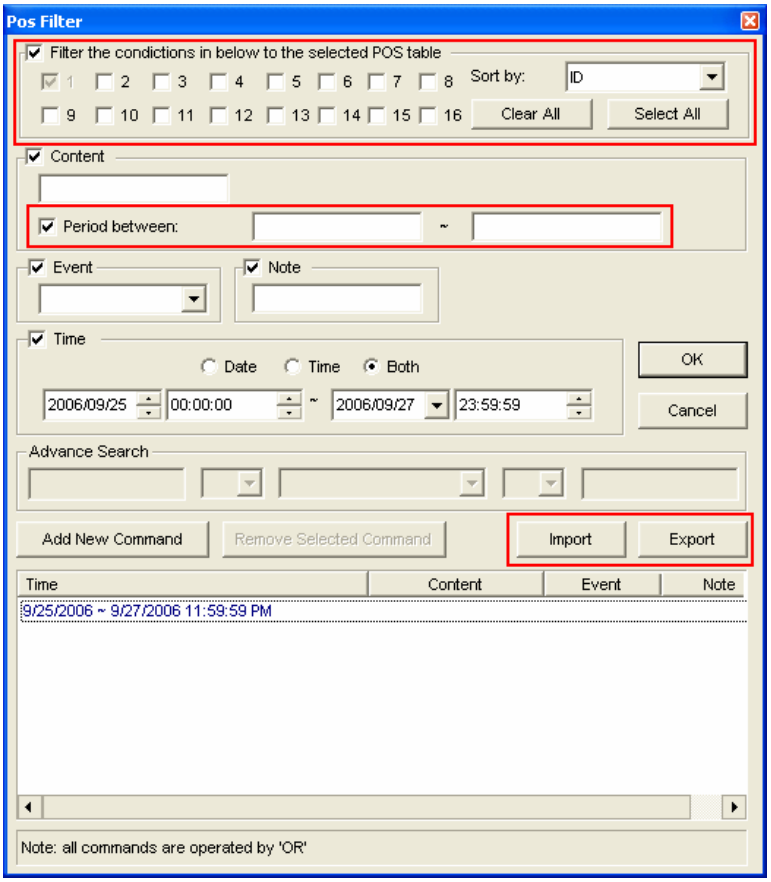


Figure 4-44

4.4 Quick Search

Quick Search is a very useful tool for searching and playing back POS events. In Advanced Log Browser (Figure 4-41), double-click any POS event in the POS table. The Quick Search window will appear. The following figure and table give you an overview on Quick Search's features and functional buttons.

Note: If the Quick Search window doesn't appear, click the **Configure** button (No. 14, Figure 1-2) on the Main System, select **General Setting** and select **System Log Setting**. Then in the POS Table drop-down list, change the video player from ViewLog to Quick Search.

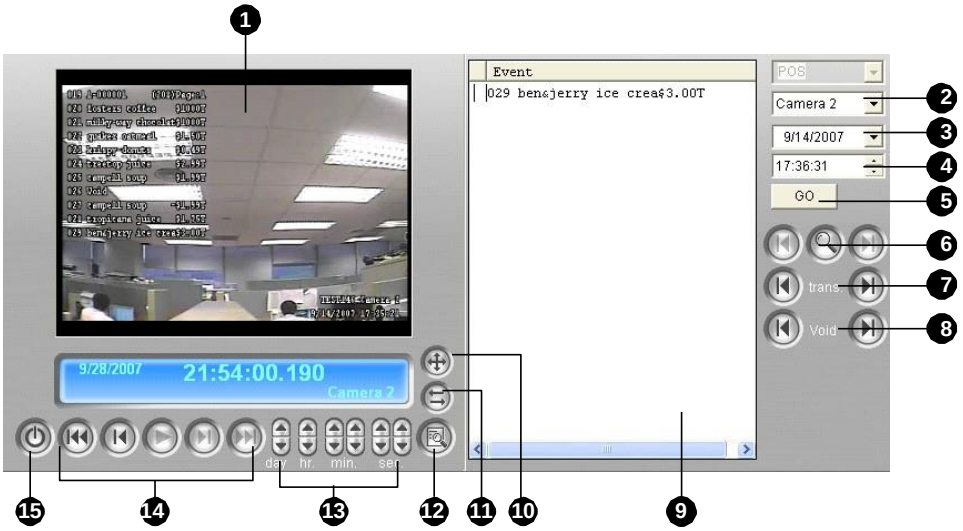


Figure 4-45 *Quick Search*

The controls on the Quick Search window:

No.	Name	Description
1	Monitoring Window	Displays video associated to the event. Right-click on the window to have the options of **Play Mode**, **Render** and **Tools**.
2	Camera Select	Use the drop-down list to select camera
3	Day Select	Use the drop-down list to select date
4	Time Select	Use the drop-down list to select time
5	Go Button	Click to search files that match to the parameters set above.
6	Event Query	Click to specify event query. See *Event Query Settings* later in this chapter.
7	Transaction	Use the arrow buttons to select previous or next transaction event.
8	Void	Use the arrow buttons to select previous or next void event.
9	Transaction Window	Displays POS transaction
10	320<->640	Click to switch between 640 x 480 and 320 x 240 display.
11	Expand / Shrink Dialog	Select **Expand/Shrink Dialog** to display the Transaction window or select **Advanced Search** to display the Advanced Search panel. See *Advanced Search Settings* later in this chapter.
12	View by ViewLog	Click to open ViewLog player.
13	Time Period	Use these buttons to search event within the specified time.
14	Playback Panel	Includes Play, Pause, Previous 10 frames, Home, Next 10 frames, End buttons.
15	Exit	Click to close Quick Search screen

4.4.1 Event Query Settings

Click the **Event Query** button (No. 6, Figure 4-45) on the Quick Search window, and the following dialog box will appear. Use this function to find POS events by a specific item, transaction, or date.

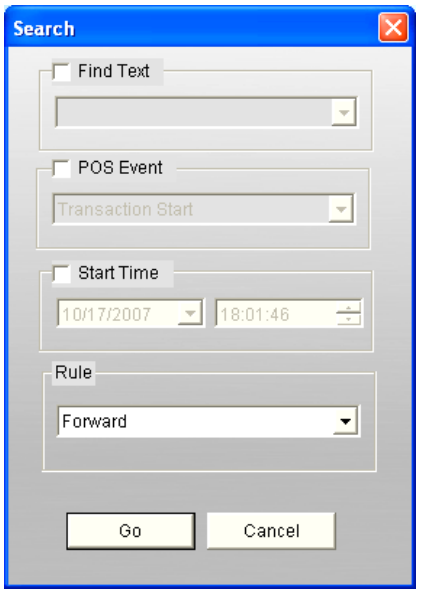


Figure 4-46

[Find Text] Enable this option to find video events that match to the key word.

[POS Event] Enable this option to find video events that match to the specified transaction type.

[Start Time] Enable this function and use the drop-down list to specify date and time

[Rule] Specify to search forward or backward from the set date.

4.4.2 Advanced Search Settings

To decide the size of Quick Search monitoring window and set up a list of favorite texts for search, follow these steps:

1. Click the **Expand/Shrink Dialog** button (No.11, Figure 4-45), and select **Advanced Search**. The Advanced Search panel appears.
2. Click the **Setting** button on the right side of the panel. This dialog box appears.

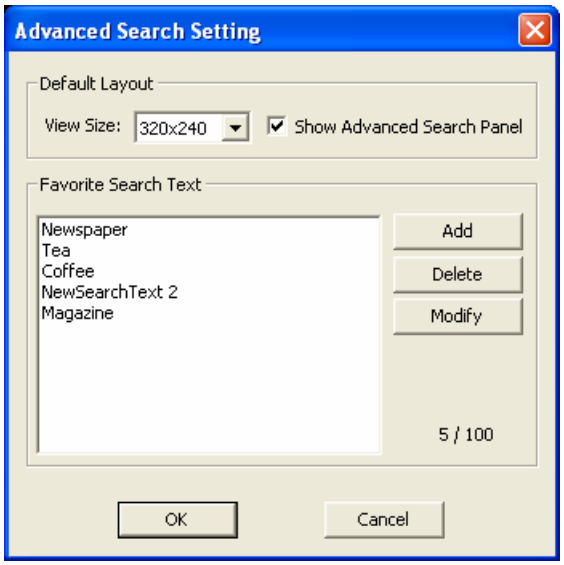


Figure 4-47

[Default Layout]

④ **View Size:** Selects 320 x 240 or 640 x 480 for the monitoring window size when the Quick Search is opened.

④ **Show Advanced Search Panel:** Displays the Advanced Search panel when the Quick Search is opened.

[Favorite Search Text]

Click the **Add** button to create a list of favorite texts for search. When you use the **Find Text** drop-down menu on the panel, this list is available for use. Up to 100 kinds of texts can be added to the list.

4.5 Address Book

With Address Book, you can save the connection information of multiple hosts and quickly access them for video playback in the future. The host you can remotely connect includes -System, IP devices, -Backup Center, -Storage System, -Recording Server, -Failover Server and -Redundant Server.

4.5.1 Creating a Host Account

To create a host account in Address Book, follow the steps below.

1. On the functional panel, click the **Tools** button and click **Address Book**. This window appears.

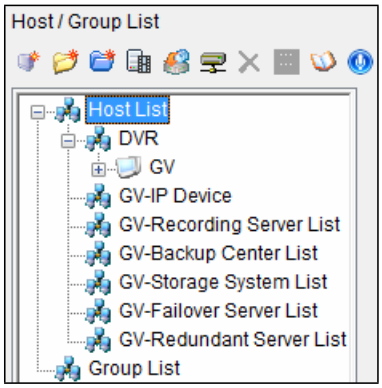


Figure 4-48

2. To add a host account, click the **Add Host** button . This dialog box appears.

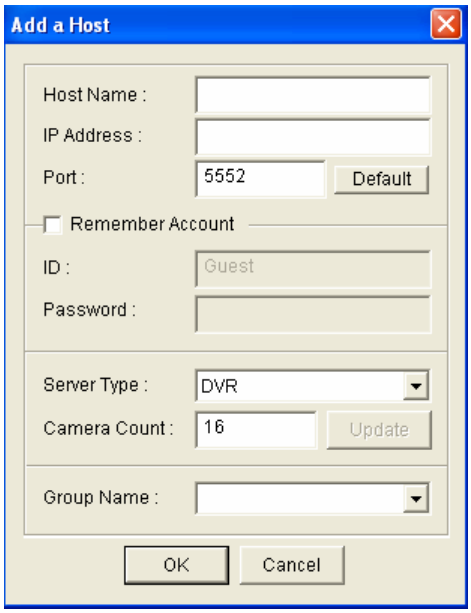


Figure 4-49

3. Type the connection information of the host, including Host Name, IP address, Port number, and login ID and Password. You can optionally select **Remember Account**, or you can enter ID and Password each time you connect the host using Address Book.
4. Select **Server Type**.
5. Click the **Update** button to request the number of cameras installed from the host.
6. Click **OK** to create the host account.

If you want to assign a group for the host, type a group name in the **Group Name** box. The group name will be added to the **Host List** and also to the **Group Name** drop-down list. Next time when you add a host, you can optionally select the created groups from the **Group Name** drop-down list.

To create a host account of -Recording Server, -Failover Server and -Redundant Server, click the **Add -Device Server** buttons. To create a host account of -Backup Center and -Storage System, click the **Add -Backup Center** and **Add -Storage System** buttons respectively. The Add a Host dialog box may look a bit different among these hosts.

Tip: Right-clicking the created host on the Address Book and selecting **Connect** can connect with the host and display its events on the ViewLog.

4.5.2 Creating a Group

You can customize a group to pull up the maximum of to 32 camera videos from different hosts directly.

1. Click the **Add Group** button.
2. Drag the desired cameras form **Host List** to the created group.

Tip: By right-clicking the created group and selecting **Connect**, images from the selected cameras will appear on the ViewLog player.

4.5.3 Creating a Folder Link

You can create a link to the folder that contains recordings from the local computer. This function has the same effect as **Reload Database** accessed from the **Advanced** button (No. 9, Figure 4-1).

⌘ To add a folder, click the **Add Folder** button, and select the video folder on the computer. The folder link is created under **Group List**.

4.5.4 Connecting from Address Book

Choose one of these ways to quickly access a host, group or folder by using Address Book:

1. Right-click a host/group/folder on Address Book, and select **Connect**.
2. Select a host/group/folder on Address Book, and select the **Connect** button .

Ensure the **Remote ViewLog** function has been enabled at the remote host to allow access from the -System.

For more remote playback functions, also see *Resuming Backup* and *Retrieving Images of Object Index* in *Remote ViewLog Service* later in this chapter.

4.5.5 Importing and Exporting the Address Book

You can import or export the address book by clicking the **Import/Export** button.

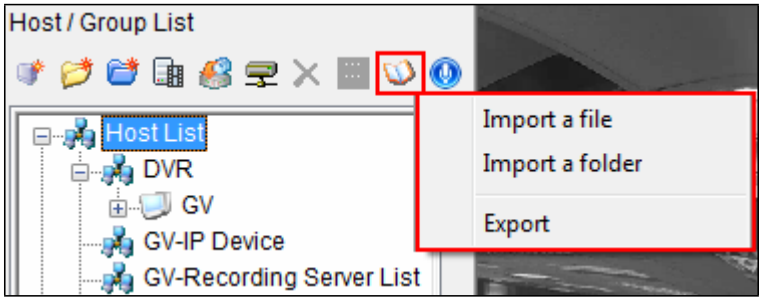


Figure 4-50

⌘ To import the address book, select **Import a file** to import a single database file of the address book. Or select **Import a folder** to simultaneously import all database files stored in the same folder.

⌘ To export the address book, click the **Export** button, and select a folder on your computer to export all database files.

Note: The database files will be divided into different types of file extensions listed as below when they are exported. You can place all the database files in the same folder, and select **Import a Folder** to import those files all at once.

File Type	Description	File Type	Description
.hd	DVR and IP Device database	.sd	Storage database
.gd	Group database	.db	Database of version earlier than V8.3.2
.rd	Backup Center database	.dat	Database of Remote Playback

4.6 Remote ViewLog Service

Through the network, you can retrieve the files from a remote IP device, -System, -Recording Server, -Failover Server, -Redundant Server or -Backup Center and play back video. This feature is made possible through the Remote ViewLog Service. The Remote ViewLog Service features:

- ⌘ Most of the functions provided by ViewLog are available, such as Backup, Save as AVI, Object Search, Export to DVD Format, Database Files Backup, and so on.
- ⌘ Capability of disabling certain camera connections under heavy network load
- ⌘ Resuming file transfers for backup

Before you can review video recorded on a remote IP device, -System, -Recording Server, -Failover Server, -Redundant Server or -Backup Center, the **Remote ViewLog** function must be enabled to allow access.

4.6.1 Retrieving Recordings from a Single Host

1. On the function panel, click the **Tools** button (No. 6, Figure 4-2), and select **Remote ViewLog Service**. This dialog box appears.

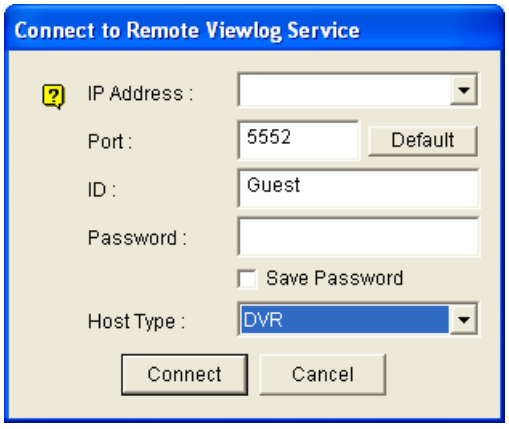


Figure 4-51

2. Enter the IP Address, ID and Password of the remote video device. Keep the default port as **5552** or modify it if necessary.
3. In the Host Type, select **DVR**, **IP Device** or **-Server**. The **-Server** option is for -Recording Server, -Failover Server, -Redundant Server and -Backup Center.
4. Click the **Connect** button.

When the connection is established, you will see the events of the remote video device appearing on the Event List. Then you can use all ViewLog features for playback.

4.6.2 Retrieving Recordings from Multiple Hosts

You can access the video files of up to 32 cameras from multiple hosts of -Systems (DVRs) and IP devices. For details, see *Creating* a *Group* earlier in this chapter.

4.6.3 Retrieving Images of Object Index

The images of Object Index include the **Object Index**, **Face Detection** and **Video Snapshot**. Through the Remote ViewLog Service, you can retrieve all the Object Index images from another -System on the network.

1. Build the connection to another -System on the network using the Remote ViewLog Service. See *Retrieving Recordings from a Single Host* earlier in this chapter.
2. Click the **Advanced** button and select **Object Index**.

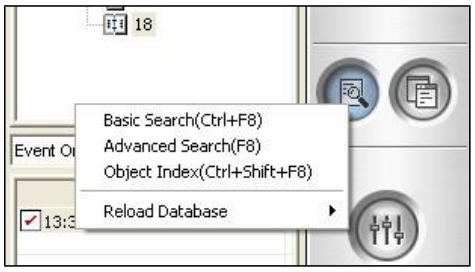


Figure 4-52

3. On the Object Index Search window, select the desired camera and file date for playback.
4. To play images with the ViewLog player, double-click the desired frame on **Object Index List**.

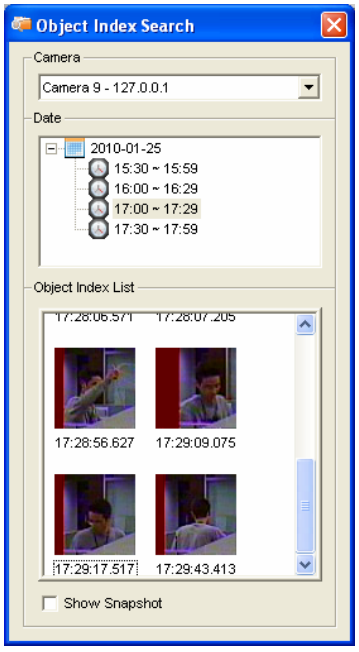


Figure 4-53

5. If you retrieve the images of **Video Snapshot**, you can select **Show Snapshot** at the bottom of the dialog box and double-click the desired frame to display it with the default image viewer of Windows, e.g. Paint.

4.6.4 Resuming Backup

Using the Remote ViewLog Service, you can back up files from a remote -System (DVR) or a IP device. When the file transfer is interrupted by a network error, you can even resume backup.

1. When the backup is interrupted, this message will appear: *There are x file(s) couldn't be backup. Do you want to keep a log file and backup them later?*
2. Click **Yes**. You will be prompted to save the partial backup file as *lv format.
3. To resume backup, click the **Resume** button in the Backup dialog box, and then locate the partial backup file to continue.

For details on backing up files, see *Chapter 5 Backup, Deletion and Repair*.

4.7 Single Player

When backing up the recorded files, you can choose to include the player of ViewLog or Single Player (see *5.2 Backing up Recorded Files*). Compared to ViewLog, the Single Player provides simple and easy playback functions. To play back the recordings using the Single Player, open the backup folder and run **SinglePlayer.exe**.

4.7.1 Single Player Window

To play back a recoded file, click **Files** and click **Open File** to select the file you wish to play back. To play back multiple recorded files together in up to 16 screen divisions, click **Files** and click **Open Folder** to select the folder that collects several camera recordings.

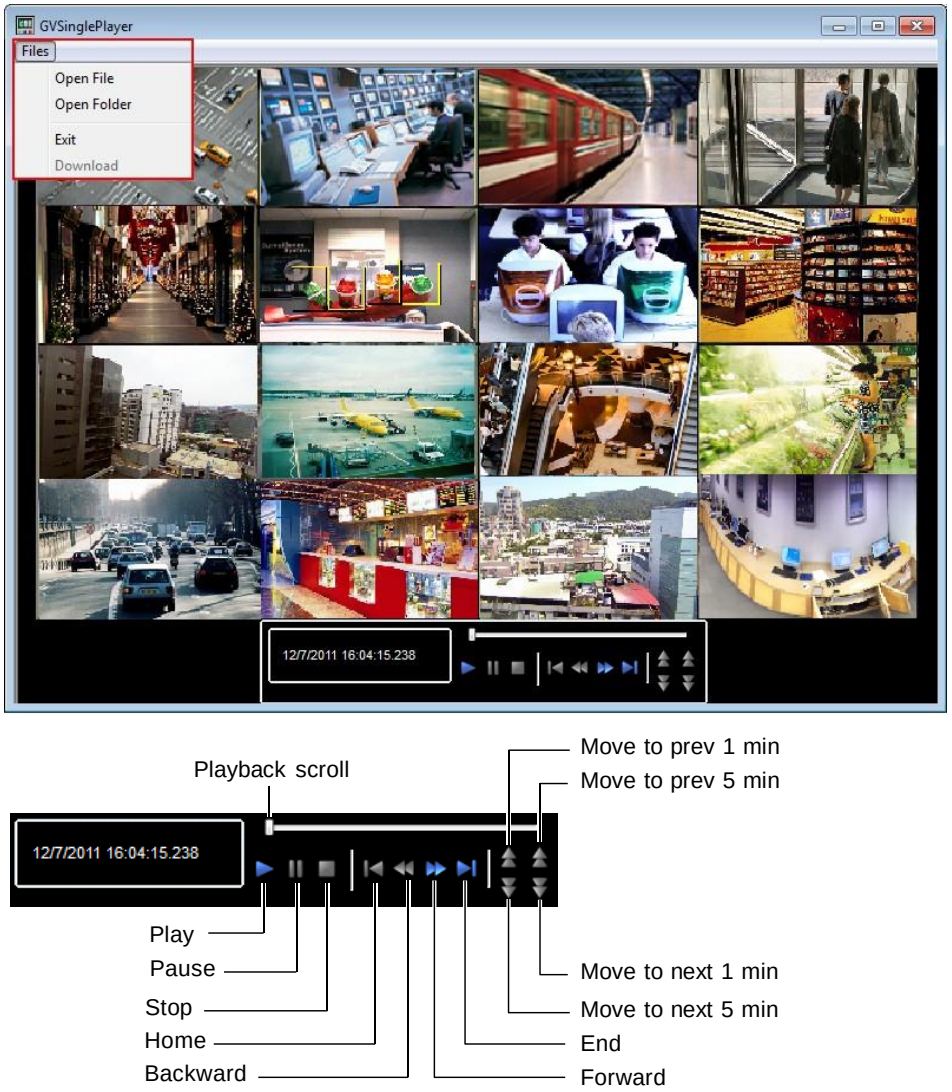


Figure 4-54

Right-clicking the playback window can change the play mode and create special effects when you play video back.

Name	Functions
Play Mode	Includes these options: ④ **Frame by Frame:** Plays back video frame by frame. ④ **Real Time:** Plays back video on real time. This mode saves waiting time for rendering, but drop frames to give the appearance of real-time playback. ④ **Key Frame:** Plays back video with key frames only. ④ **Smooth Playbacks:** Evenly distributes 30 frames per second. When the playback appears choppy, select this option to enhance the smoothness. ④ **Auto Play Next 5 Minutes:** Plays back video up to 5 minutes. ④ **Audio:** Turns on or off the video sound; audio denoise.
Render	Includes these options: ④ **Deinterlace:** Converts the interlaced video into non-interlaced video. ④ **Scaling:** Smoothens mosaic squares when enlarging a playback video. ④ **Deblocking:** Removes the block-like artifacts from low-quality and highly compressed video. ④ **Defog:** Enhances image visibility. ④ **Stabilizer:** Reduces camera shake. ④ **Text overlay's camera name and time:** Overlays camera name and time onto the video. ④ **Text overlay's POS/ -Wiegand:** Overlays POS or -Wiegand Capture data onto the video. ④ **Wide angle lens dewarping:** Corrects distortion toward the corner of the camera view. ④ **Fisheye:** Select Geo Fisheye to choose a camera mode. ④ **Mega Pixel View:** Enables PIP or PAP view. ④ **Display GPS:** Shows the location on the map where the video is taken through GPS. ④ **Select GPS Map (Apply after restart):** Select a type of GPS map to apply. ④ **Full Screen:** Switches to the full screen view.
Tools	④ **Snapshot:** Saves a video image. ④ **Save as AVI:** Saves a video as avi format. ④ **Download:** Downloads the video clip from the DVR or video server to the local computer.

4.8 GPS Tracks Playback

Since -Video Server and -Compact DVR support GPS tracking, GPS tracks are recorded along with video on these devices. On the -System, you can retrieve GPS tracks from these devices and play them back in Google Maps, Microsoft Virtual Earth and even user-defined maps.

1. IP device must allow the remote access with **ViewLog Server** activated. See *ViewLog Server* in its user's manual.
2. To remotely connect to IP device from -System, click the **Tools** button and select **Remote ViewLog Service**. The Connect to Remote ViewLog Service dialog box appears.
3. Enter the connection information of IP device, and click **Connect**. Once the connection is established, the video events will be displayed on the Video Event list.
4. To select a map API (Application Program Interface), click the **Tools** button and click **Select Map API**. This dialog box appears.

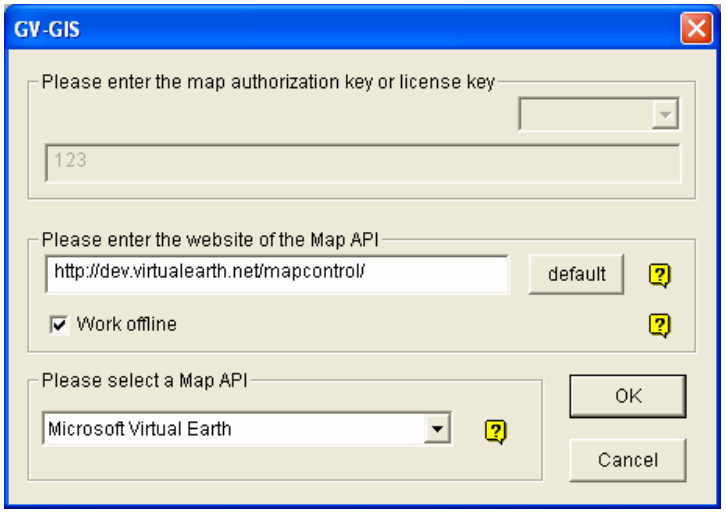


Figure 4-55

5. In **Please Select a Map API**, select a Map API.
6. To play back GPS tracks, click the **Tools** button and select **Display GIS** Window. The first-time user will be prompted for a License Agreement. Read through the license terms before you click **I understand and agree** to continue.

7. Select the events with GPS tracks from the Video Event list, select the desired video mode, and click the **Play** button to start.

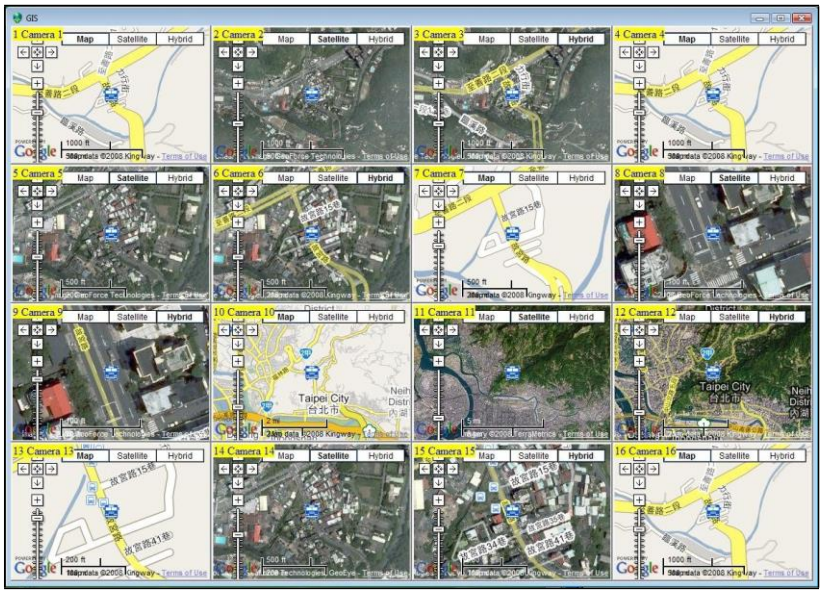


Figure 4-56

Note:

1. If you like to use the maps created yourself, overwrite the files at :\ folder\GIShtm-User, and select **User Defined** from the “Please Select a Map API” drop-down list (Figure 4-55).
2. You can also attach the USB mass storage device with the recorded files to -System for playback. For this kind of playback, first load the data to ViewLog by following the instructions in the section of *Playback Using USB Mass Storage Device* in -Video Server or -Compact DVR User’s Manual. Then follow Steps 4-7 above to play back GPS tracks.

4.9 Touch Screen Support

By the touch of a finger, the touch screen panel allows you to change screen divisions, switch to full screen and close the ViewLog screen.

1. Click the **Tools** button (No.6, Figure 4-2), point to **Tool Kit**, select **Touch Screen Panel**, and click **Panel Setup**. This dialog box appears.

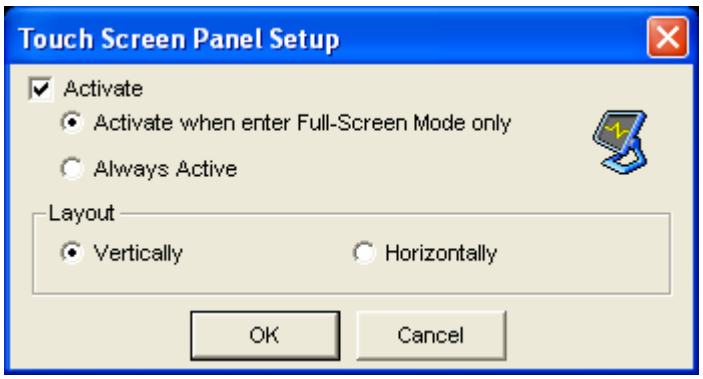


Figure 4-57

2. Click **Active** to have these options:

   ④ **Active when enter Full-Screen Mode only:** Launches automatically the panel when the full screen view is applied.

   ④ **Always Active:** Always displays on the ViewLog screen.

   ④ **Layout:** Select a vertical or horizontal panel.

3. Click **OK** for the above settings.
4. At the upper left corner of the screen, an information window indicating date, time and storage space will appear. Left-click it to open this touch panel.

Figure 4-58

4.10 Fast Key Reference

To view the fast key list, click the **Tools** button (No.6, Figure 4-2), point to **Took Kit**, and then select **Fast Key**. The ViewLog fast key list appears.

4.11 Specifications

Feature	Notes
Support for Defogging	Yes (32 channels)
Support for Stabilizer	Yes (32 channels)
Support for PIP View	Yes
Support for PAP View	Yes
Support for Panorama View	Yes (4 sets of Panorama View)
Videos Exported as .AVE Files	Yes
Object Search	Yes
Support for Fisheye View	Yes

Chapter 5

Backup, Deletion and Repair 301

5.1 Backing Up Log Data..... 301

5.2 Backing Up Recorded Files 303

5.3 Splitting Backup Files onto Multiple Discs..... 306

5.3.1 Excluding the Player in the Backup Files..... 306

5.3.2 Including the Player in the Backup Files..... 308

5.4 Deleting Recorded Files..... 309

5.5 Repairing Damaged File Paths 311

5.6 Repairing Damaged Video Files 313

CHAPTER

5

Backup, Deletion and Repair

This chapter explains how to back up and delete video/audio files. Video files can be copied from the hard disk to external storage media, such as CD-R, DVD, MO, or ZIP drives. Video files saved on the hard disk can be deleted as well.

5.1 Backing Up Log Data

Using the System Log, you can back up all log data or filtered data based on criteria.

1. To open the System Log, click the **ViewLog** button on the main screen (No.13, Figure 1-2), and select **System Log.**
2. Click the icon at the top left corner on the System Log window, and select **Advanced Log Browser**. The Advanced Log Browser appears.
3. Select a time period of logs to be loaded to the Advanced Log Browser.
4. Click the **Backup** button on the toolbar. This dialog box appears.

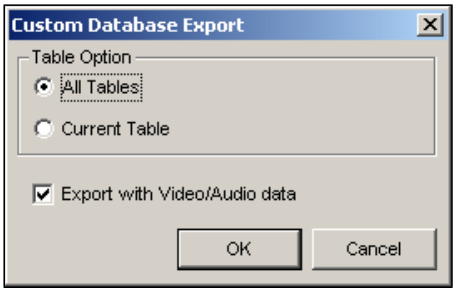


Figure 5-1

[Table Option]

④ **All Tables:** Backs up all log data.

④ **Current Table:** Backs up only the log table you are currently at.

[Export with Video/Audio data] Backs up video/audio attachments with log data.

5. Click **OK**. The Backup dialog box (Figure 5-2) appears.
6. In the Media section, select the method and destination to back up the log files.
7. Click **OK** to back up.

Note:

1. To back up the filtered data, use the **Filter** function to define search criteria first. See *Filter Settings* in the section of *Advanced Log Browser* in Chapter 4.
2. To open the backup data, run **EZSysLog.exe** from the backup file.

5.2 Backing Up Recorded Files

Using ViewLog, you have three backup options:

⌘ Back up to hard disk

⌘ Create CD/DVD using a third-party software, e.g. Nero, Roxio, etc.

⌘ Create CD using Windows XP / Vista / Windows 7 / 8 / Windows Server 2012 inbuilt burning software.

To back up files:

1. On the function panel, click the **Backup** button (No. 7, Figure 4-2). This dialog box appears.

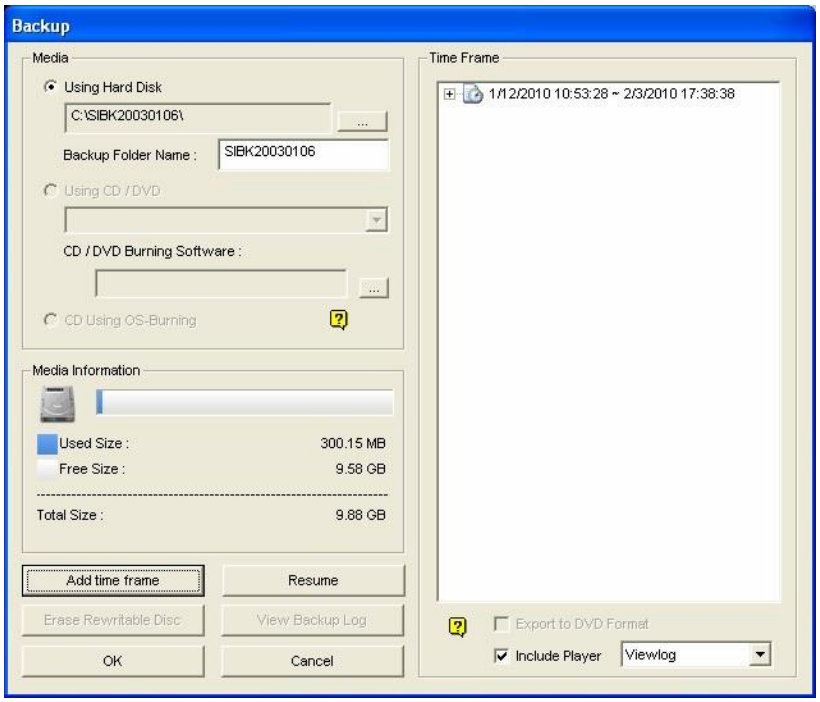


Figure 5-2

2. Select a destination media to back up files.

[Media]

④ **Using Hard Disk:** Click to back up files to the hard disk you select. Click the **[…]** button to select the desired hard disk.

④ **Backup Folder Name:** Enter a desired name for the backup folder.

④ **Using CD/DVD:** Click to back up files to the CD or DVD media using the third-party software.

🕘 Click the **[…]** button to assign the desired burning software (.exe file). When you click **OK** on the Backup dialog box (Figure 5-2), the system will ask you to paste the backup files to the CDR-Writer program, and call up the assigned burning software for you to paste and backup files.

- If Nero software of version 6.6.0.14 or later is installed, the backup feature provides the direct burn function. It allows you to directly burn the files onto CD/DVD without the need to assign the burning software and pasting the backup files to the CDR-Writer program.
- If Nero software of version 7.0 or later is installed, the backup feature allows you to directly burn the files to blue-ray media.

④ **Using OS-Burning:** This option is only available when you use Windows XP, Vista or Windows 7 / 8 / Windows Server 2012. It burns files using the inbuilt software of the operation system onto the DVD, CD or blue-ray disc. Note that your hard disk needs at least 1 G buffer space.

[Media Information] This section indicates free and used space on CD/DVD media or the local disk.

3. Click the **Add Time Frame** button to define a time period for backup.

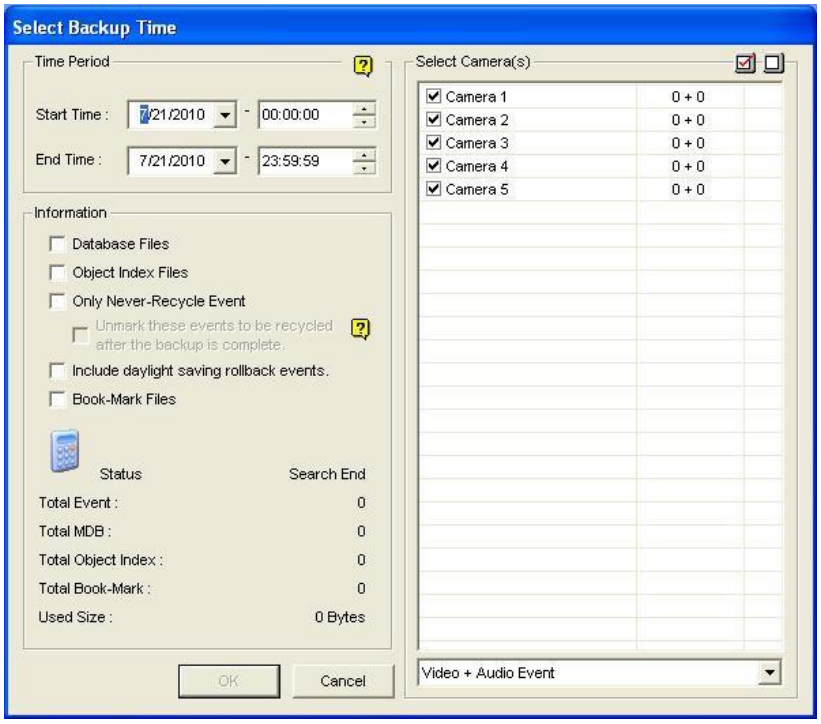


Figure 5-3

[Time Period] Specify the time periods for backup.

[Select Camera(s)] Click to select the camera(s) for backup. The number of video and audio files of each camera is indicated respectively, e.g. “Camera 1 1+0” means Camera 1 has 1 video file and 0 audio file.

④ **Video + Audio drop-down list:** Select the types of video events for backup.

[Information]

- ④ **Database Files:** Click to back up the files from System Log.
- ④ **Object Index:** Click to back up the Object Index files.
- ④ **Only Never-Recycle Event:** Click to only back up the never-recycle events.
- ④ **Unmark these events to be recycled after the backup is complete:** After the backup is complete, the never-recycle events will be unmarked for recycling. Please note if the first file in the database has been marked and then unmarked in this condition, the first file will be deleted automatically.
- ④ **Include daylight saving rollback events:** Click to back up events recorded during Daylight Saving Time.
- ④ **Bookmarked Files:** Click to back up the bookmarked frames in JPEG format.
- ④ **The Status and Search End section:** Indicates the number of backup files and their total size. (Total MDB refers to the System Log files.)

4. Click **OK** to add the schedule. You can repeat step 3 to create up to 10 periods of time.
5. To include the player to the backup files, select **Include Player** at the right bottom of the Backup dialog box and select **ViewLog** or **Single Player**. By default, **ViewLog** is selected. If no player is selected, you can only play the backup files at the computer installed with -System or Geo Mpeg4 codec.
6. Click **OK** on the Backup dialog box to start the backup.

Tip: If you just want to back up a specific event or several events of one day, select the event or multiple events on the Video Event list, and right-click to select **Backup**. The Select Backup Time dialog box will then appear, and you can follow the steps described above to back up files without setting up the time period.

Note:

1. If you are unable to record a CD, make sure the CD recording is enabled in your CD burner: open **My Computer**, right-click the CD Drive icon, click **Properties**, click the **Recording** tab, and then check **Enable CD recording on the drive**.
2. The **Export to DVD Format** option, at the right bottom of the Backup dialog box (Figure 5-2), outputs your files in DVD movie format, meaning that it will play in any DVD player that supports writable DVD disks. To enable this option, MPEG2 files recorded by the -2004 Card / -2008 Card need to be selected first (see the Select Camera(s) option), and a DVD±RW disk is required as well.
3. For ViewLog and Single Player, see *Chapter 4 Video Playback*.

5.3 Splitting Backup Files onto Multiple Discs

When the size of the backup files exceeds the disc space limit, the ViewLog can automatically split the files to be burned onto multiple discs. For this feature to work, **Nero 6.6.0.14** or later is required to be installed on your system.

Note: This feature is not available when

1. the **Export to DVD Format** option is enabled to back up files to DVD, or
2. the **CD Using OS-Burning** option is enabled to back up files using the inbuilt burning software of the operating system.

To back up files, click the **Backup** button (No. 7, Figure 4-2), and follow the instructions in the *Backing Up Files Using ViewLog* section earlier in this chapter. When the system splits backup files into multiple discs, two backup modes are selectable. The backup modes change when you exclude or include the player in the backup files. For details on the two backup modes, see the following sections.

5.3.1 Excluding the Player in the Backup Files

If you choose not to include the player in the backup files, there are two backup modes:

⌘ **Mode 1:** This mode intelligently burns files onto CD/DVD by shifting the complete event(s) to a new CD/DVD if space is not enough on the current CD/DVD. You may see some blue screen images at the beginning or the end of each CD/DVD.

1. When you start burning, a dialog box appears.

Figure 5-4

2. For Mode 1, select **No**. A dialog box indicating the number of required discs for burning appears.

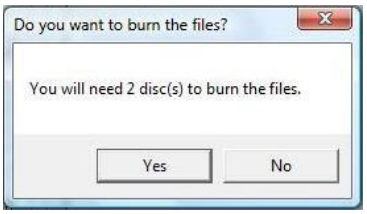


Figure 5-5

3. Select **Yes** to start the backup.

⌘ **Mode 2:** This mode will keep some buffers at the end and beginning of each CD/DVD, thus overlapping some videos in the beginning of each CD/DVD from the end of the previous CD/DVD.

1. When you start burning, a dialog box (Figure 5-4) appears.
2. For Mode 2, select **Yes**. A dialog box indicating the number of required discs for burning (Figure 5-5) appears.
3. Select **Yes** to start the backup.

5.3.2 Including the Player in the Backup Files

If you choose to include the player in the backup files, the **Model 2** backup method will be applied. You may see some overlapping videos in the beginning of each CD/DVD from the end of the previous CD/DVD.

1. To include the player in backup files, select **Include Player** at the right bottom of the Backup dialog box, and select **ViewLog** or **Single Player**.

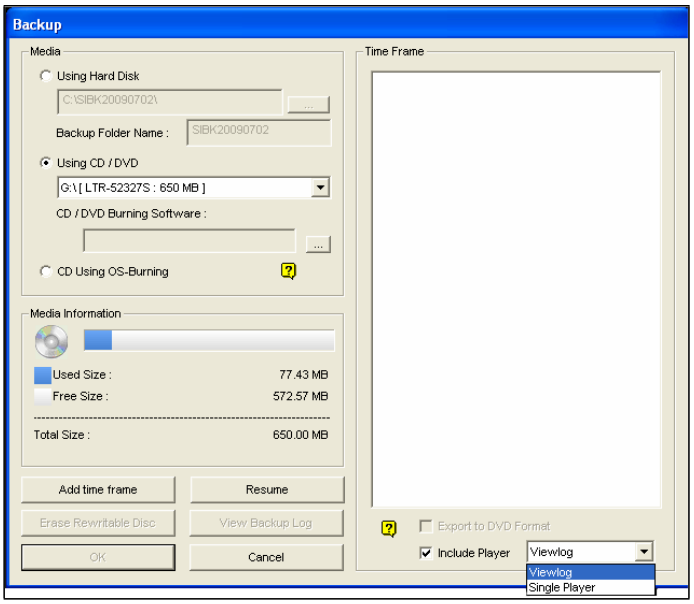


Figure 5-6

2. When the backup process starts, a dialog box indicating the number of discs required for backup appears.
3. Click **Yes** to start the backup.

5.4 Deleting Recorded Files

To delete files using ViewLog, follow these steps:

1. On the function panel, click the **Tools** button (No. 6, Figure 4-2), and select **Delete Log**. This dialog box appears.

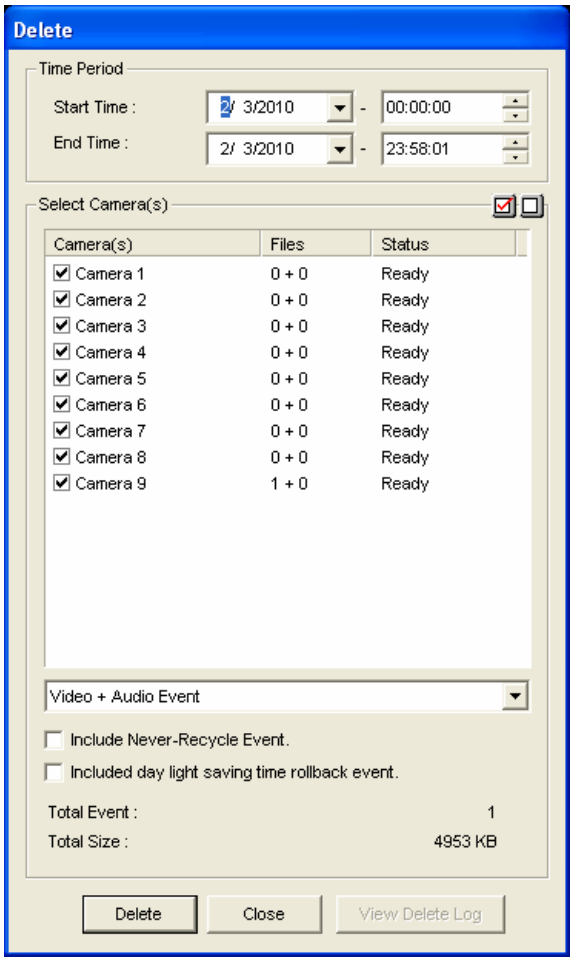


Figure 5-7

2. Define the time period for file deletion.
3. Uncheck the cameras, which you don't want to delete the files of.
4. Use the drop-down list to select the types of events to be deleted, e.g. video, audio or both together.
5. If you want to delete the never-recycle events, select **Include Never-Recycle Event**.
6. If you want to delete the events recorded during the Daylight Saving Time period, select **Included Day Light Saving Time Rollback Event**.
7. Click the **Delete** button.

Tip: If you just want to delete a specific event or several events within one day, select the event or multiple events on the Video Event list, and right-click to select **Delete**. The Delete dialog box will then appear, and you can follow the steps described above to delete files without setting up the time period

.

Note:

1. If you want to view the history of file deletion, click the **View Delete Log** button on the Delete dialog box.
2. To view the information of files from a desired camera, right-click the camera and select **Event View** on the Delete dialog box.

5.5 Repairing Damaged File Paths

The only way to correctly delete video and audio files is through the operation you've just performed in the previous section. If you move or delete a video file using Windows Explorer or Windows File Manager, the -System will not know what you have done. In this case, the Repair Database Utility can repair misplaced or missing recorded files that are not identified by the ViewLog player. As long as these files still exits on the hard drives and detectable by Windows operating system, the Utility will restore these recorded files back to their default paths and allow them to appear under ViewLog. This Utility comes with the installation of Main System. Follow these steps to repair the paths:

1. Go to the **Windows Start** menu, select **Programs**, select the folder, and select the **Repair Database Utility**. The valid ID and password are required.
2. When the Select Camera for Repair Database dialog box appears, select the cameras that require database repair.
3. Click **OK**. This dialog box appears.

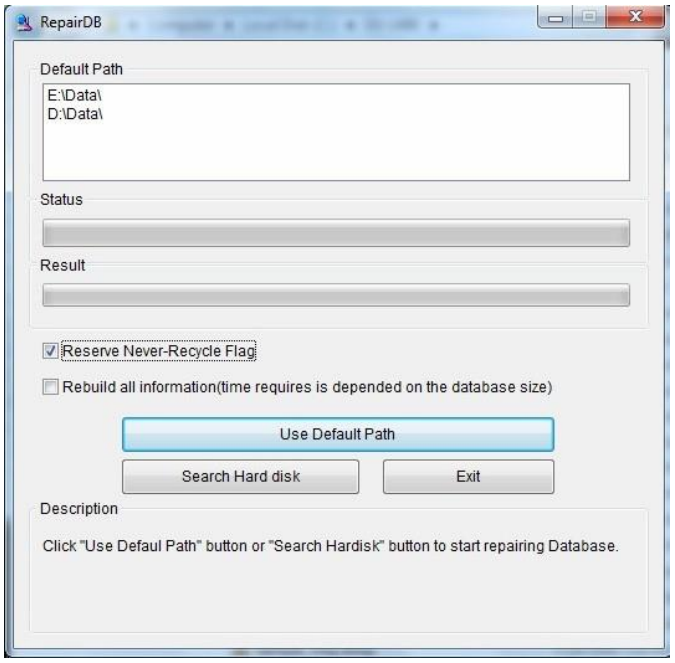


Figure 5-8 *The RepairDB Dialog Box*

4. If your recorded files exist only in the predefined recording paths, click the **Use Default Path** button. The -System will rebuild paths for these files in the predefined recording hard drives only.
5. If your recorded files scatter across different hard drives, click the **Search Hard Disk** button. The -System will rebuild paths for these recorded files in all hard drives connected to the -System. In this way, more time will be required for building the database.

Note:

1. The repair and the search function will not apply to the files that have been renamed manually.
2. Use this Utility if encountering any of the following scenarios in ViewLog:
   a. A question mark appears right before a video file in the Video Event list.
   b. When you click the **Playback** button, no video is displayed even a file is selected.

5.6 Repairing Damaged Video Files

If the computer has been shut down improperly, e.g. due to power failure, use this function to repair the damaged video files.

Tip: When a computer has been shut down improperly, the first thing you do before starting the -System is to run **Repair Database Utility**. After running the Utility, go back to ViewLog and view Video Events. You should be able to play back all video files at this step. However, if what you see is a question mark after clicking on the file, the problem may be that the recording process was interrupted. To repair the file, run the AVI Repair Utility and follow the steps below.

---

1. Double-click **AVIRepairAPI.exe** in the folder. This dialog box appears.

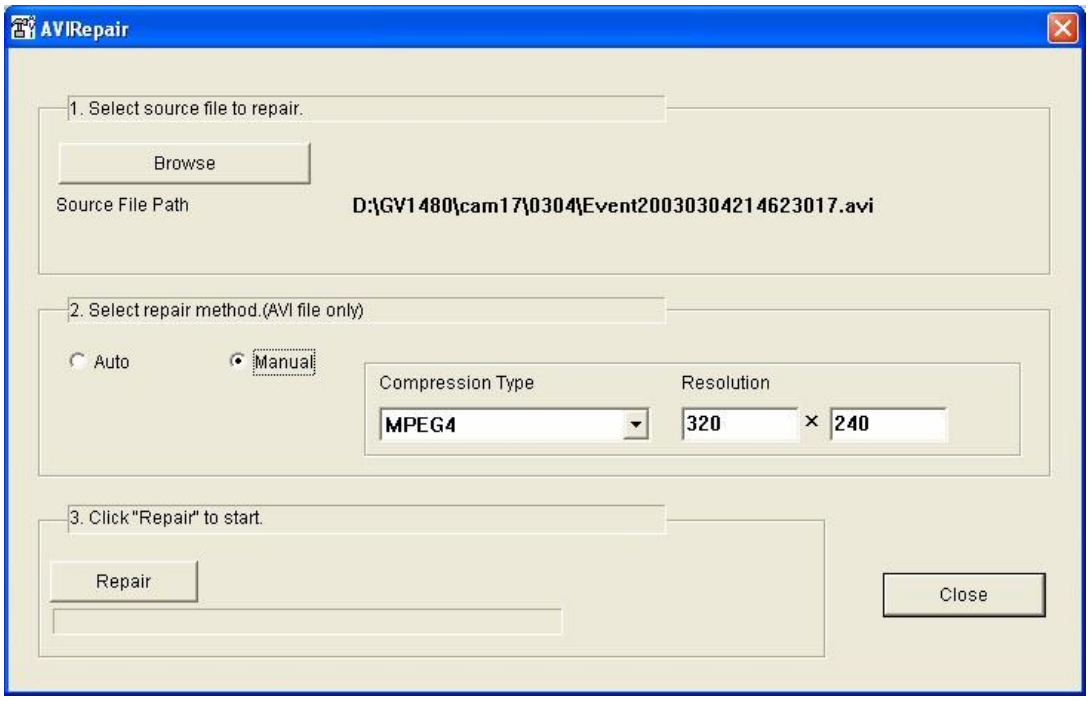


Figure 5-9

2. Click the **Browse** button to find the damaged video file.
3. If you know the codec and resolution of the file, select **Manual**, select **Compression Type** and type **Resolution**. Alternatively, you may select **Auto** and the system will run all combinations for you. Please note it takes longer time to repair with this selection.
4. Click the **Repair** button to start.

5. You may see the distorted image or **No Image** on view screen if an incorrect codec and resolution were chosen. For this, click **No** for the next combination until a complete image appears.

Distorted Image

Figure 5-10

No Image

Figure 5-11

Complete Image

Figure 5-12

6. When a complete image is displayed, click the arrow button to preview the file.
7. Click **Yes** to start the repair.
8. Click **Yes** to overwrite or **No** to save this file to another path. Note if you choose **No** in this step, remember to run **Repair Database Utility** again after exiting this program.

Chapter 6

I/O Applications 316

6.1 I/O Device Setup 317

6.1.1 Latch Trigger 319

6.1.2 Keeping Last Toggle Status 321

6.2 I/O Control Panel 323

6.3 Advanced I/O Applications 324

6.3.1 Setting Up Actions Upon Input Trigger 325

6.3.2 Moving PTZ Camera to a Preset Location upon Input Trigger 327

6.3.3 Setting Momentary and Maintained Modes 328

6.3.4 Deactivating Alarm and Alert Settings upon Input Trigger 329

6.3.5 Overlaying Input Name onto Screen upon Input Trigger 330

6.4 Input State Detection 331

6.5 I/O Enable Setting 332

6.6 Advanced I/O Panel 333

6.6.1 The Advanced I/O Panel 333

6.6.2 Creating a Group for Cascade Triggers 334

6.6.3 Configuring the Advanced I/O Panel 337

6.6.4 Setting Up Mode Schedule 338

6.6.5 Quick Link 340

6.6.6 Forcing Output 341

6.6.7 Editing Background Image 342

6.6.8 System-Wide Triggers 343

6.6.9 The “Advanced Logical Input Status in Multicam” Option 344

6.6.10 Managing a Group of I/O Devices 345

6.7 Visual Automation 346

6.7.1 Setting Visual Automation 346

6.7.2 Using Visual Automation 347

6.8 Virtual I/O Control 348

6.8.1 Setting a Module 349

CHAPTER

6

I/O Applications

This chapter discusses how you can set up and control the I/O devices connected to -System. I/O applications include these features:

- ⌘ Configure I/O devices
- ⌘ Move PTZ to a preset location on input trigger
- ⌘ Support access control systems of Momentary and Maintained modes
- ⌘ Arm and disarm I/O devices without interfering with the monitoring
- ⌘ Centrally manage I/O devices across the wide area by the Advanced I/O Panel

6.1 I/O Device Setup

To connect the I/O device to the computer of -System, you may need the additional device: -Net, -Net Card, -NET/IO Card or -I/O Box. For details on these devices, see Chapter 2 in the *-DVR and Accessories Installation Guide* on the Software DVD.

To install the I/O device on the -System, on the main screen, click the **Configure** button (No. 14, Figure 1-2), select **Accessories**, select **I/O Device** and click **I/O Device Setup**. This window appears.

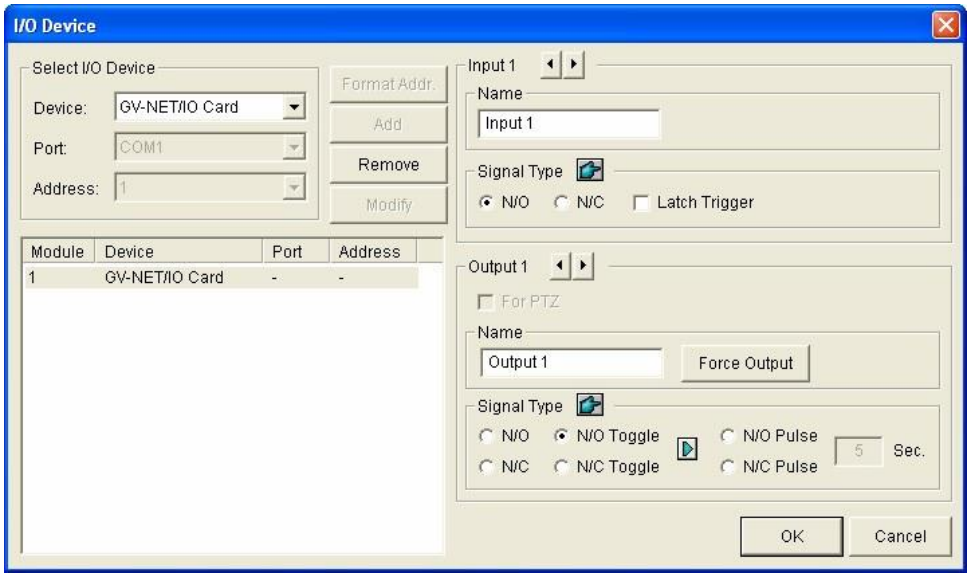


Figure 6-1 *I/O Settings*

[Select I/O Device] Adds an I/O device to the system:

1. Select the device from the **Device** drop-down list.
2. Click the **Format Addr.** button to assign an address to the device. The Format Address dialog box appears.
3. Start your first device with **New Address** set to 1. Click the **Write** button to write the address to the device. Click **OK** to apply the setting.
4. Click the **Add** button. You should see the device listed in the display window.
5. Repeat above steps to add more devices once at a time. Each device should have its own address; therefore, in step 3 you should assign a different address for the new device.

Note: For -Net/IO Card V3.1 (Net/IO Card Mode), select the **-NET/IO Card** option; for -Net/IO Card V3.1 (I/O Box Mode) and -I/O Box 4 Ports, select the **IO-USB(4)** option; for -IO Box 8 Ports, select the **IO-USB(8)** option, and for -I/O Box 16 Ports, select the **IO-USB(16)** option.

[Input X] Click the **Arrow** buttons to select an Input to set up.

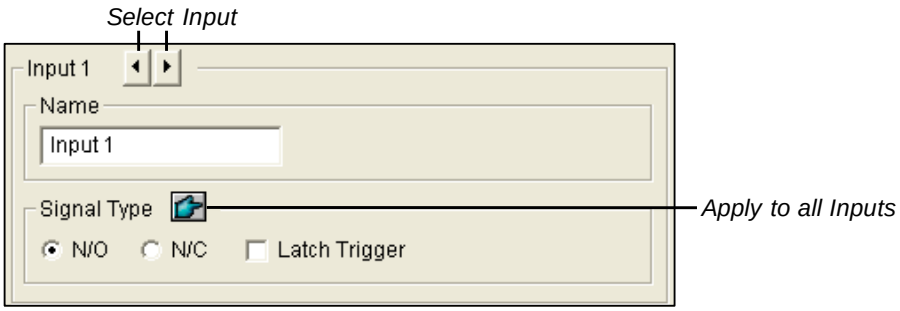


Figure 6-2

④ **Name:** Specifies a name for the input device in the Name field.

④ **Signal Type:** Select a signal type for your input device: NO (normally open), NC (normally close) or Latch Trigger. Clicking the finger button can apply your selection to all input devices.

For details on Latch Trigger, see *Latch Trigger* later in this chapter.

[Output X] Click the **Arrow** buttons to select an output.

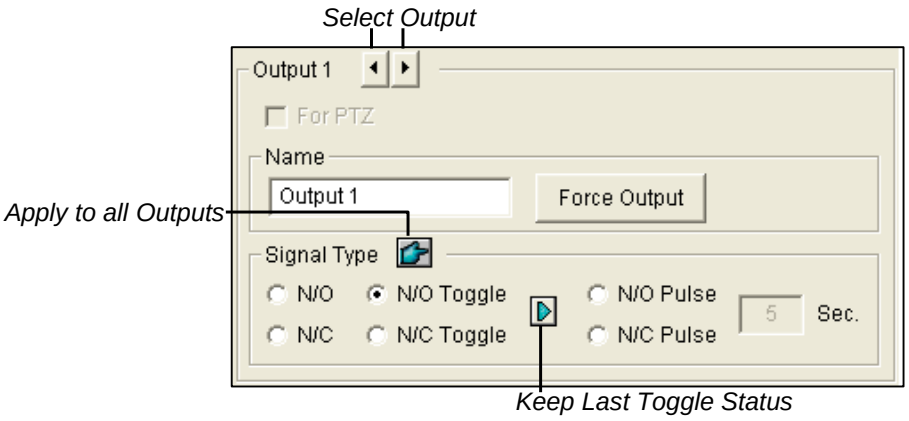


Figure 6-3

④ **Name:** Specifies a name for the output device in the Name field.

④ **Force Output:** Click to test signal to the selected device.

④ **Signal Type:** There are six signal types available: N/O (Normal Open), N/O Toggle, N/O Pulse, N/C (Normal Closed), N/C Toggle, and N/C Pulse. Choose the one that mostly suits the device you're using. For **Toggle** output type, the output continues to be triggered until a new input trigger ends the output. For **Pulse** output type, the output is triggered for the amount of time you specify in Sec field.

④ **Keep Last Toggle Status:** See *Keeping Last Toggle Status* later in this chapter.

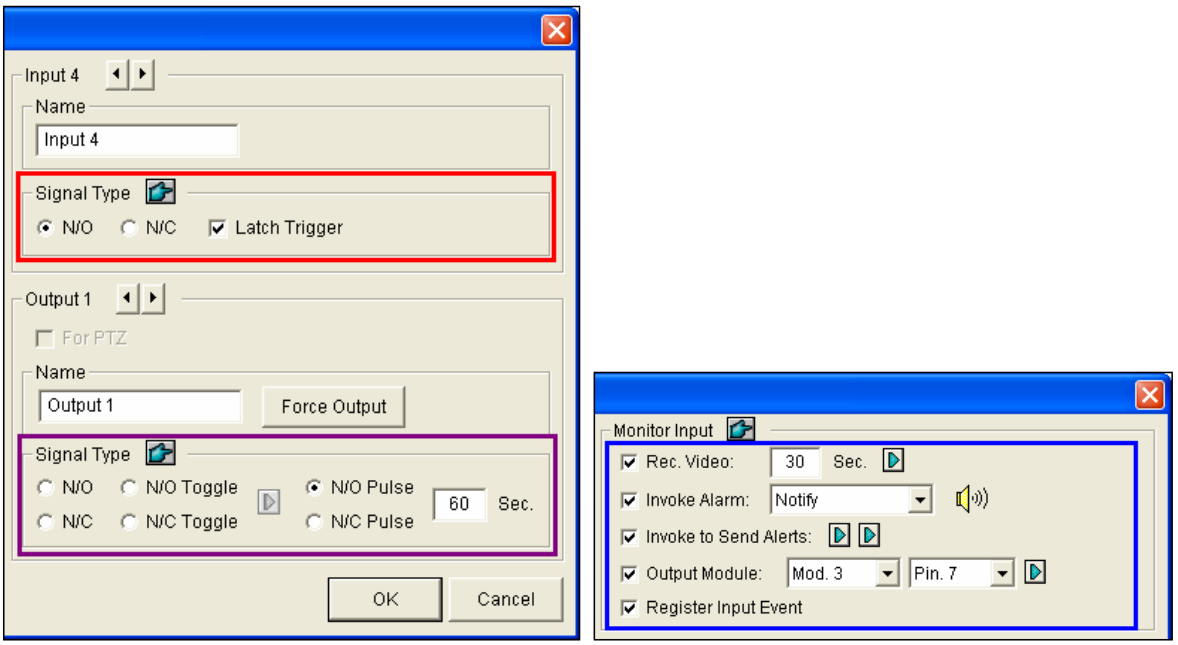
Note: PTZ camera and I/O devices cannot be assigned to the same port at the same time.

6.1.1 Latch Trigger

Instead of constant output alarm in N/O and N/C, the Latch Trigger option provides a momentary alarm, and allows you to set the alarm duration.

Setting up Latch Trigger:

On the main screen, click the **Configure** button (No. 14, Figure 1-2), point to **Accessories**, click **I/O Device**, and select **I/O Device Setup** to select the **Latch Trigger** option. See the red square in the dialog box below.



I/O Device Setup *I/O Application Setting*

Figure 6-4

Application Example:

In the above scenario, Input 4 is set to N/O and Latch Trigger as well. When Input 4 is triggered:

⌘ The camera starts recording for 30 seconds and stops itself until the next input trigger (see the Rec Video option in the blue box).

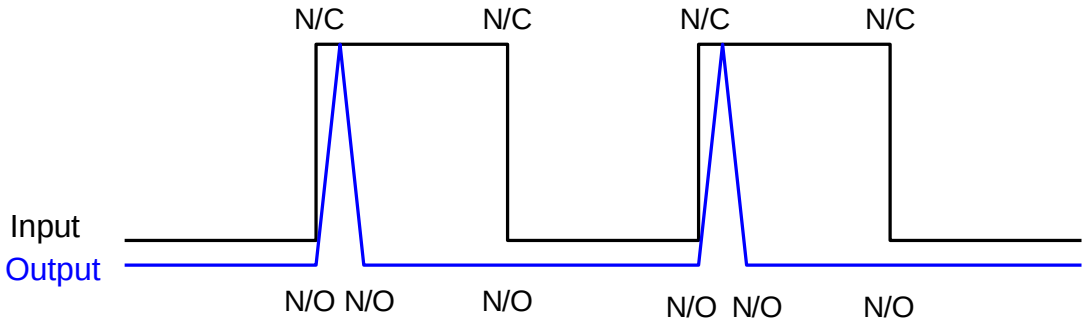
⌘ Computer Alarm sounds once (see the Invoke Alarm option).

⌘ The output (Module 3, Pin 7) is triggered simultaneously based on the Latch Trigger mode (see the illustrations below).

The following illustrations can help you understand different output signals (see Purple Square in the above dialog box) working with the Latch Trigger option.

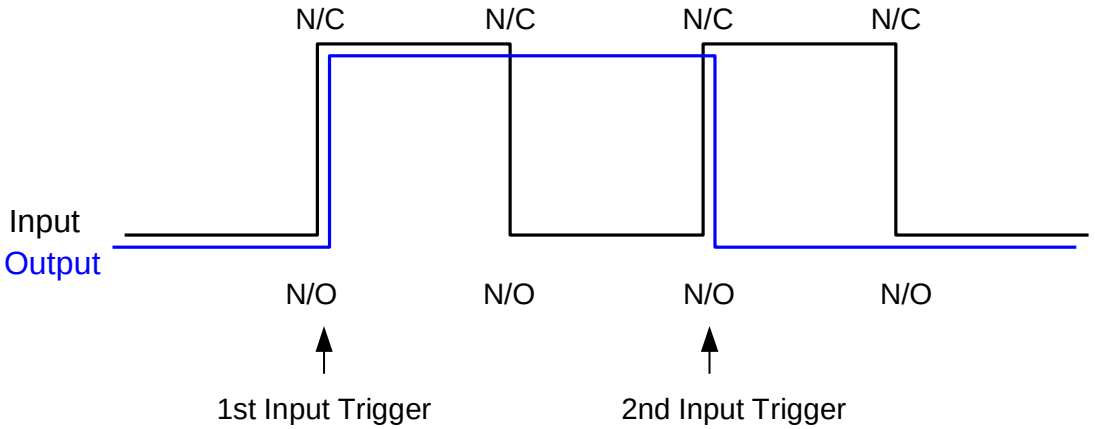
1. N/O (Normal Open) + Latch Trigger

Once the input triggers the output, the output will be triggered for a short moment and then turn off itself.



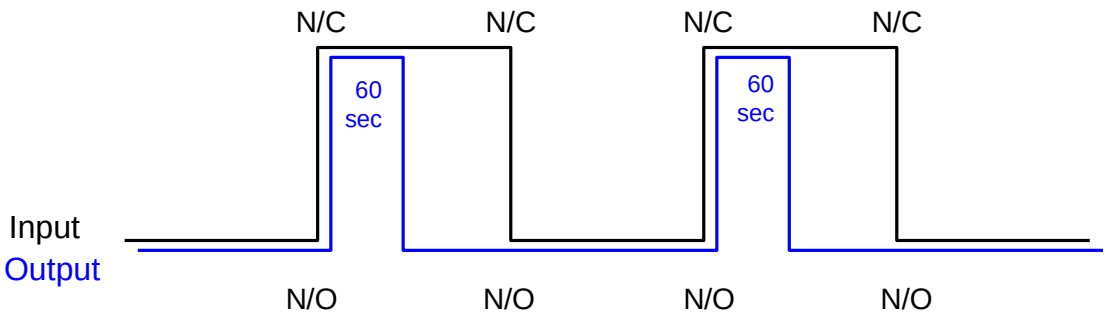
2. N/O Toggle + Latch Trigger

Once the input triggers the output, the output will keep triggering until a new input trigger.



3. N/O Pulse + Latch Trigger

Suppose you set the Pulse time to 60 second. Once the input triggers the output, the output will remain ON for 60 seconds before turning off itself.



6.1.2 Keeping Last Toggle Status

This feature can memorize the current output state when the monitoring is stopped or the system is restarted. For example, suppose the output is lights. When remaining on the premises, you stop monitoring but the triggered lights remain ON, not affected by the system state.

Setting up “Keep Last Toggle Status”:

In the I/O Device dialog box (Figure 6-1), select **N/O Toggle** or **N/C Toggle**, and click the **Arrow** button beside to check **Keep Last Toggle Status**.

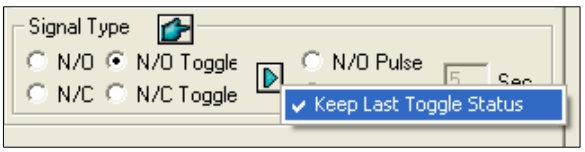


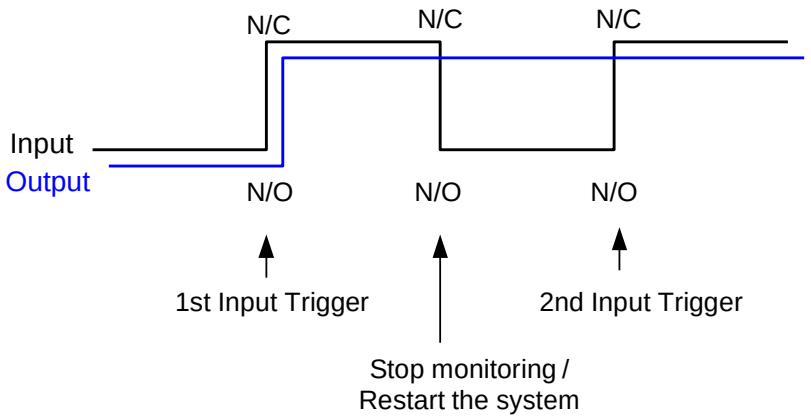
Figure 6-5

Application Example:

Following two illustrations help you understand how the input works with the output set to **Keep Last Toggle Status**.

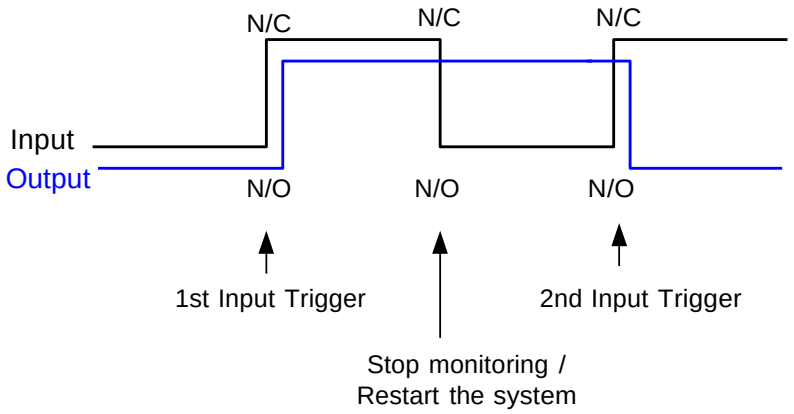
1. Input (N/O) + Output (N/O Toggle + Keep Last Toggle Status)

The triggered output remains ON even when you stop monitoring or restart the system.



2. Input (N/O + Latch Trigger) + Output (N/O Toggle + Keep Last Toggle Status)

When “Latch Trigger” works with “Keep Last Toggle Status”, the output only has a momentary trigger but also needs to remain ON even when you stop monitoring or restart the system. Therefore under the two conditions, the output turns off until a new input trigger.



6.2 I/O Control Panel

The I/O control panel is used to control I/O devices that are added to the system. This control panel will not appear, unless at least one I/O device is connected to the system. To add and to configure a device, see *I/O Device Setup* earlier in this chapter.

After a device is added to the system, click the **I/O** button on the main screen to bring out the on-screen control panel for inputs and outputs (Figure 6-6). If only one I/O device is connected to the system, click the **I/O** button and select **Module 1** to bring up the control panel; if more than one I/O modules are connected to the system, clicking the **I/O** button will list all I/O modules connected to the system. Select one to bring out the control panel.

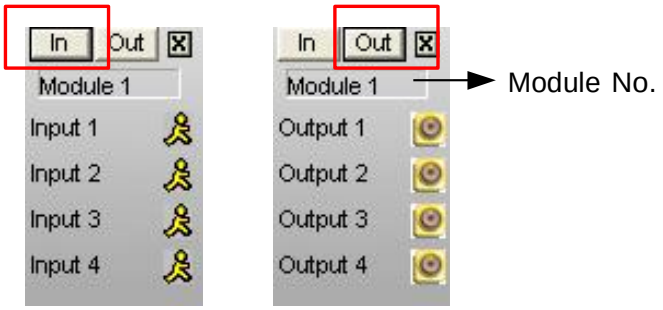


Figure 6-6

- **Input Control Panel:** Displays the status of current input sensors. The “walking man” icon indicates the sensor is being triggered.
- **Output Control Panel:** Displays the status of current output devices. You can force the output device to be triggered by clicking on its icon.

6.3 Advanced I/O Applications

In the I/O Application dialog box, you can configure the advanced applications, such as setting alarm notification, defining a PTZ camera movement upon input trigger, setting momentary or maintained mode, and deactivating alarm and alert settings. Click the **Configure** button (No. 14, Figure 1-2), point to **Accessories**, click **I/O Application**, and select **I/O Application Setting**. This dialog box appears.

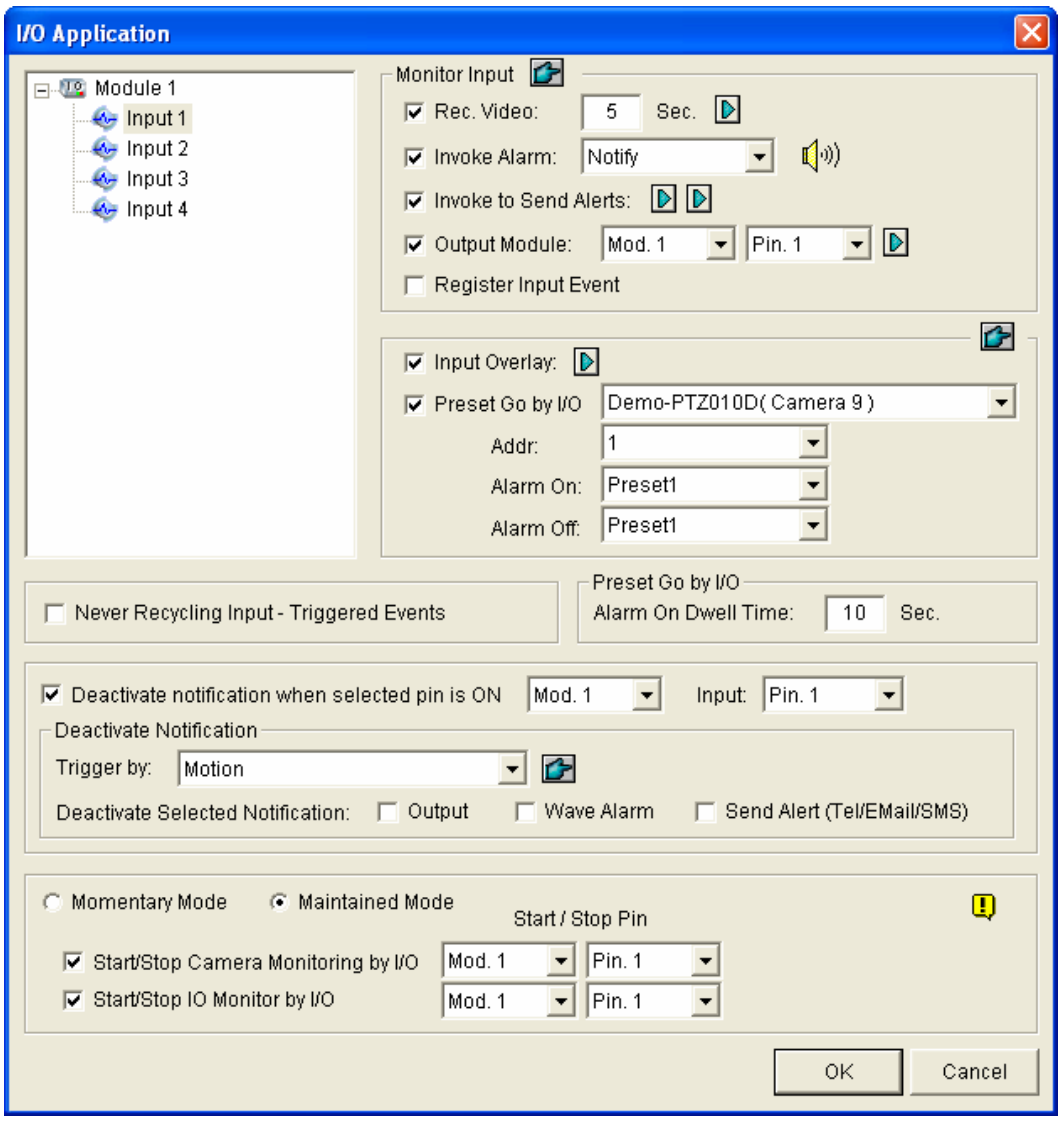


Figure 6-7 *I/O Application*

6.3.1 Setting Up Actions Upon Input Trigger

This section helps you set up the actions to be taken after the input device is triggered and whether to recycle input-triggered events or not.

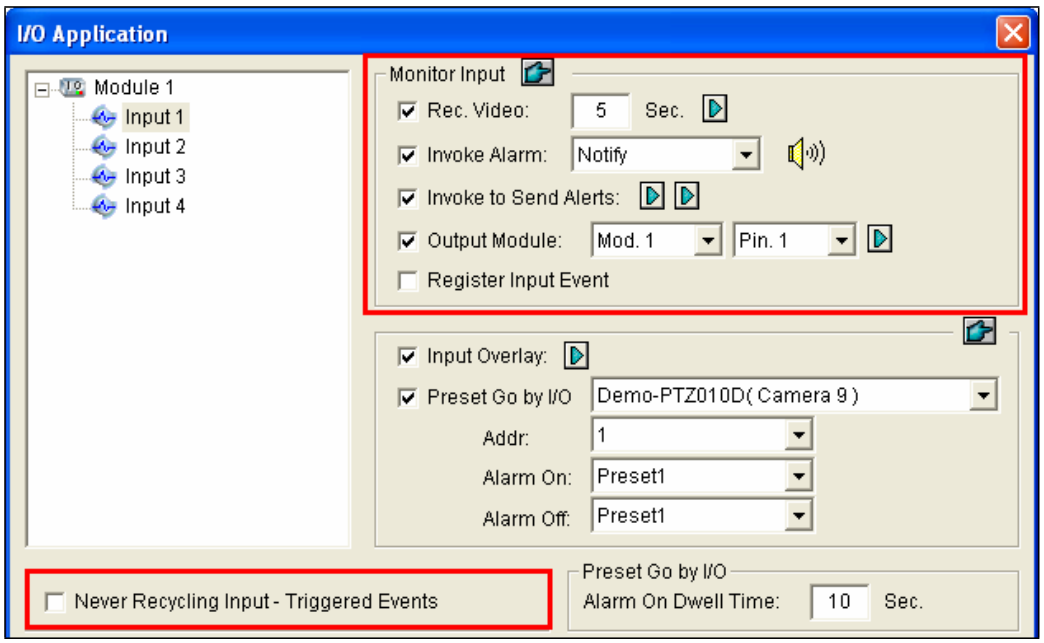


Figure 6-8

Select an Input number to be set up. Clicking the Finger button can apply the same settings to all inputs.

[Monitor Input]

④ **Rec Video:** Select this option to use the input (sensors or detectors) to trigger recordings on multiple cameras. Specify the recording duration and click the **Arrow** button to select which camera to record upon input trigger.

④ **Invoke Alarm:** Select this option to activate computer alarm when the input is triggered. You can select the alarm sound from the drop-down list.

④ **Invoke to Send Alerts:** Select this option to send out the predefined alert (E-Mail/Hotline/SMS) when the input is triggered. For e-mail alerts, see *E-Mail Notification* in Chapter 1; for hotline alerts, see *Hotline Notification* in Chapter1; for SMS alerts, see *Short Message Service* in Chapter 10.

1st Right Arrow button: Appears when E-Mail is the predefined alert. Click the button to select the camera(s) to take a snapshot upon input trigger. The snapshot will be sent out by E-Mail.

2nd Right Arrow button: Sets the time to delay the activation of assigned alerts (E-Mail/Hotline/SMS).

④ **Output Module:** Triggers the specified output module when the input is activated. Use the drop-down lists to select the output module and pin number to perform this function.

Right Arrow button: Sets the time to delay the activation of the specified output module.

④ **Register Input Event:** This option logs the I/O trigger events into System Log. Each event is labeled with ID, time, device name (camera or I/O input), corresponding module of the device, and event for later retrieval. For details on System Log, see *System Log* in Chapter 1.

Note: The Delay Time in **Invoke to Send Alerts** and **Output Module** allow you time to turn off the input device before the system triggers alerts or the output device. The Delay Time will not work if you stop monitoring or enable the function "**Deactivate notification when selected pin ON**" in I/O Application window (Figure 6-7).

[Never Recycling Input-Triggered Events] When the item is checked, the recorded files of input-triggered events won't be recycled by the system when disk space is full.

6.3.2 Moving PTZ Camera to a Preset Location upon Input Trigger

This feature allows you to define how the PTZ camera and the -System will respond to an input trigger event.

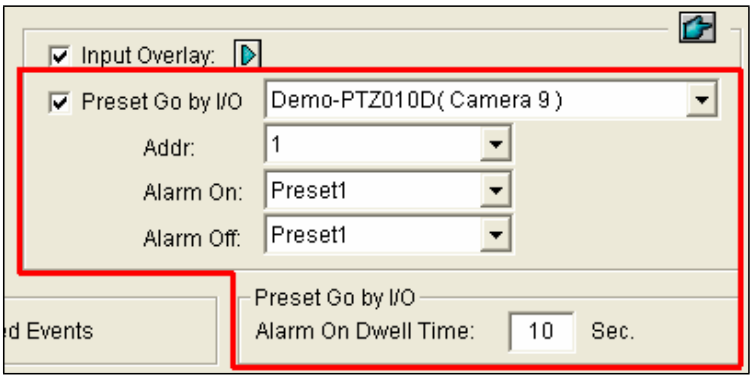


Figure 6-9

Select an Input number to be set up. Clicking the Finger button can apply the same settings to all inputs.

④ **Preset Go by I/O:** Enable the option and select your PTZ camera from the drop-down list.

④ **Addr:** Specify the address of the PTZ camera.

④ **Alarm On:** Turns the PTZ camera to a preset point when the input is triggered.

④ **Alarm Off:** Returns the PTZ camera to a preset point when the triggered input is off.

④ **Alarm On Dwell Time:** Specify the amount of time the PTZ camera stays at “Alarm On” preset point, before returning to the “Alarm Off” preset point.

Note: Depending on the capability of the PTZ camera, up to 256 PTZ preset points (ranging from 1 to 256) and addresses (ranging from 0 to 255) can be programmed.

6.3.3 Setting Momentary and Maintained Modes

This section introduces the momentary and maintained modes.

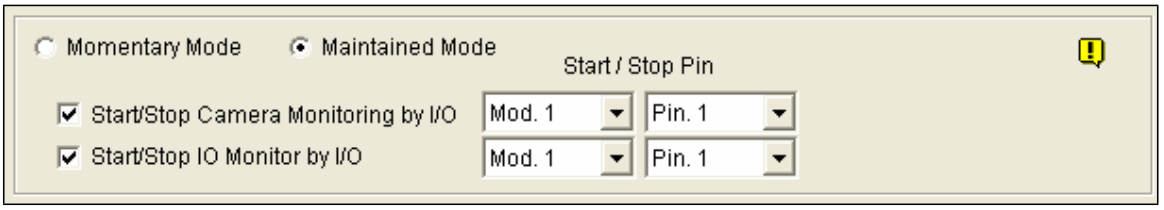


Figure 6-10

[Momentary Mode] Pushbutton switches that are normally open and stay closed only as long as the button is pressed. Momentary switches allow turn-on or turn-off from multiple locations. For example, certain premises have a designated entry/exit door. When the staff enters the entry door, the system starts monitoring. When the staff leaves from the exit door, the system stops monitoring.

[Maintained Mode] Push-on/push off button switches that stay open until thrown, and then stay closed until thrown again. Maintained switches are convenient for only one switch location.
For example, in the business hour when the door is opened, the system stops monitoring; in the non-business hour when the door is closed, the system starts monitoring.

6.3.4 Deactivating Alarm and Alert Settings upon Input Trigger

The option lets you instantly deactivate all the prior alarm and alert settings (Output, Wave Alarm, Send Alerts), when an assigned input module is triggered.

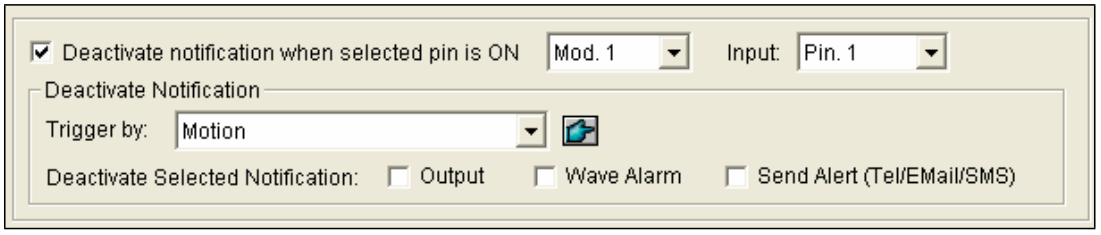


Figure 6-11

[Deactivate notification when selected pin is ON] When an assigned input module is activated, all designated alarms and alerts will be disabled. Assign an installed input module and a pin number for the application.

[Deactivate Notification]

④ **Triggered by:** Select an alert condition from the drop-down list for the application. For example, if you choose Motion, all designated alarms and alerts upon motion detection will be deactivated when the assigned input module is activated.

④ **Deactivate Selected Notification:** Select the alarms and alerts you want to be deactivated, such as Output, Wave Alarm and/or Send Alert, when the assigned input module is activated.

6.3.5 Overlaying Input Name onto Screen upon Input Trigger

This feature is designed to overlay the name of input device on live video for alert or save it to video files whenever the input is triggered.

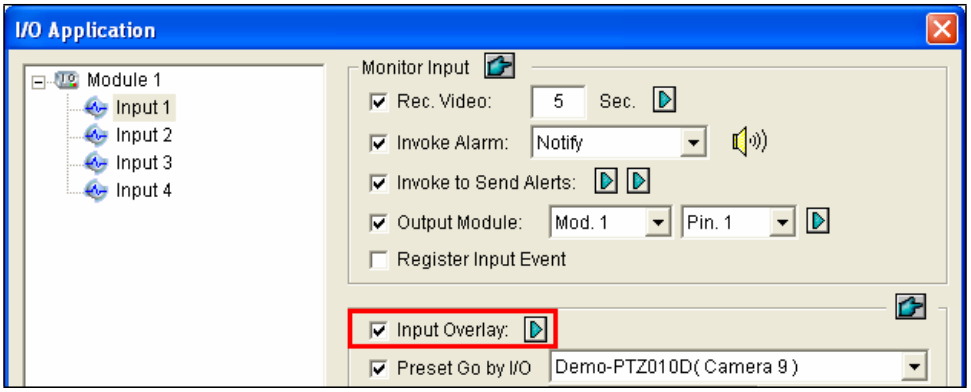


Figure 6-12

Select an Input number to be set up. Clicking the Finger button can apply the same settings to all inputs. The input name can be found and modified in Figure 6-1.

[I/O Overlay] Click **Setup** to display this dialog box, use the drop-down lists to select the input module and pin number, and then select camera(s) associated with the input device..

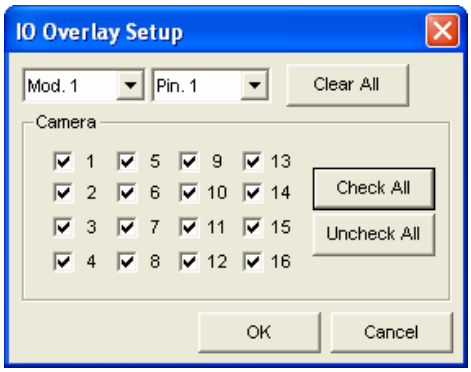


Figure 6-13

To overlay the name of triggered input on live video, click the **Configure** button (No. 14 , Figure 1-2), select **General Setting**, select **Text Overlay Setting**, and select **Print on screen (Only for I/O alarm)** or **Print on video file**. You can also select the position of the name stamp on the screen. For details, see *POS Data Overlay* in Chapter 7.

Note: Up to 5 input names can be stamped on each channel when inputs are triggered.

6.4 Input State Detection

This feature is designed to monitor all inputs for a change of state whenever you start I/O monitoring. A change from the defined state (N/O to N/C or N/C to N/O) can activate an alarm condition, e.g. a warning light or buzzer.

1. On the main screen, click the **I/O** button (No. 7, Figure 1-2), and select **Detect Input Status**. This dialog box appears.

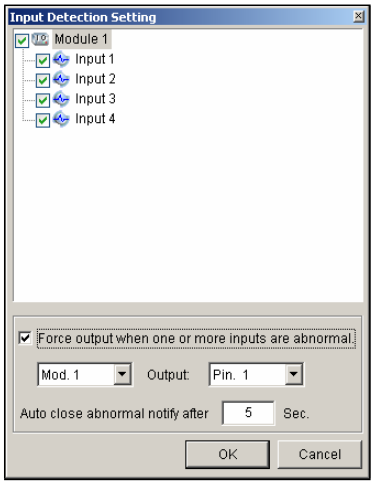


Figure 6-14

2. Check the Input(s) you want to monitor.
3. For any state change, you can trigger an alarm output by checking **Force Output when one or more inputs are abnormal**, and assigning the output module and pin number.
4. When the state change is detected, a warning message will pop up on the screen. In the **Auto close abnormal notify after x sec** field, you can define the duration of the message to close itself automatically.

After settings, you can manually detect all input states by selecting **Detect Input Status**. Or, you can just start I/O monitoring. When the system detects any change of input state, you may see this warning message:

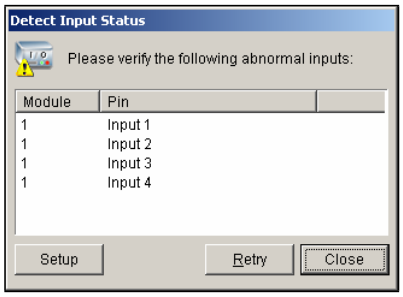


Figure 6-15

6.5 I/O Enable Setting

You can manually arm or disarm any I/O devices without interrupting the monitoring. For example, when an output alarm is triggered at the front door, you can turn off the output while the system keeps on recording and I/O monitoring.

Arming / Disarming I/O devices:

1. On the main screen, click the I/O button (No. 7, Figure 1-2), and select **I/O Enable Setting**. This dialog box appears.

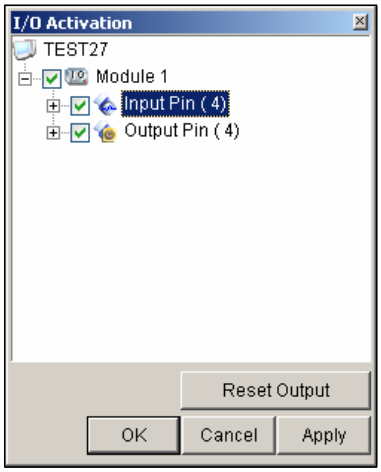


Figure 6-16

2. Check the Input/Output to arm or uncheck the Input/Output to disarm the device(s). Then click **Apply** to verify the changes.

6.6 Advanced I/O Panel

The Advanced I/O Panel provides a centrally managing solution for I/O devices installed across a wide area. It simplifies the process of configuring and managing many I/O devices. Its major features are:

- ⌘ Trigger I/O devices without starting I/O monitoring
- ⌘ Group I/O devices for cascade triggers
- ⌘ Monitor different I/O cascade configurations at different times of the day
- ⌘ Quickly access triggered I/O devices by a Quick Link window

6.6.1 The Advanced I/O Panel

To open the panel, click the **I/O** button on the main screen, and then select **Advanced I/O Panel**.

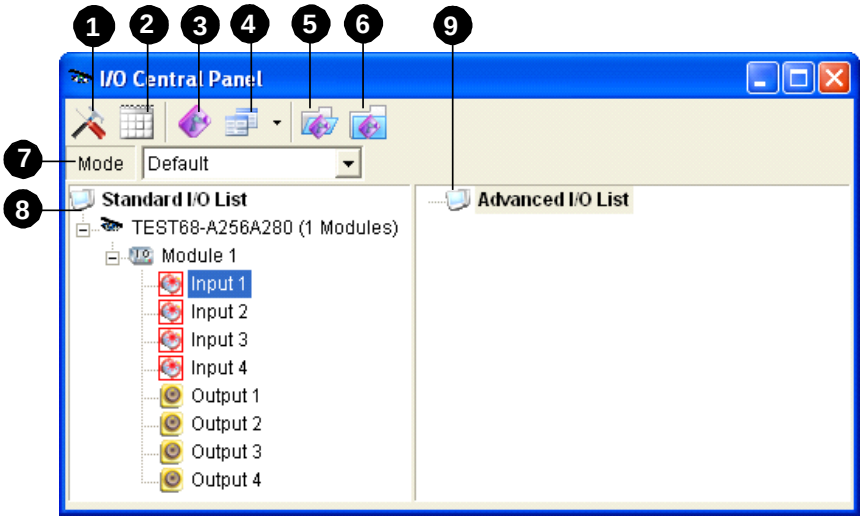


Figure 6-17

The controls on the Advanced I/O Panel:

No.	Name	Description
1	Configure	Accesses Panel and Schedule settings.
2	Mode Schedule	Starts/stops Mode Schedule.
3	Toggle Quick Link	Displays the Quick Link window for quick access to triggered I/O devices.
4	Advanced I/O List Style	Displays the Advanced I/O List in various styles: View/Edit, Icon and Detail.
5	Expand Tree Row	Expands tree branches.
6	Collapse Tree Row	Collapses tree branches.
7	Mode	Configures various cascade modes.
8	Standard I/O List	Displays connected I/O modules.
9	Advanced I/O List	Groups I/O devices in cascade mode.

6.6.2 Creating a Group for Cascade Triggers

You can group I/O devices by function or geography. Further, the group allows cascade triggers, meaning that the trigger actions of one trigger can activate another trigger.

For example, you might have a group called “Entrance” that contains all I/O devices installed at entrances. The “Entrance” group might contain other sub groups, each of which contains just the related I/O devices in various geographic locations:

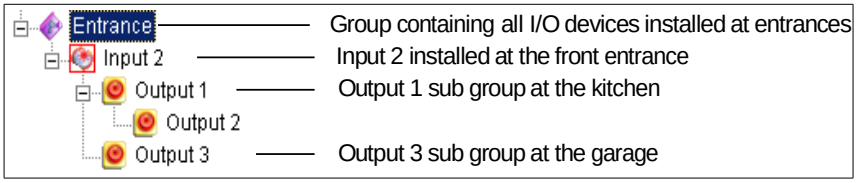

Entrance
Group containing all I/O devices installed at entrances
Input 2
Input 2 installed at the front entrance
Output 1
Output 1 sub group at the kitchen
Output 2
Output 3
Output 3 sub group at the garage

Figure 6-18

When Input 2 is triggered, it will trigger the sub groups of Output 1 and Output 3, and Output 1 will trigger Output 2 in a cascade series.

Creating a Group:

1. Right-click on **Advanced I/O List**, and then select **Add A Group**. This dialog box appears.

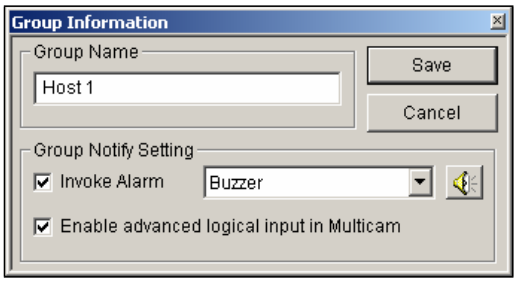


Figure 6-19

④ **Group Name:** Names the group.

④ **Invoke Alarm:** Invokes the computer alarm on I/O trigger. Select a sound from the drop-down list.

④ **Enable advanced logical input in Multicam:** See *The “Advanced Logical Input Status in Multicam” Option* later in this chapter.

2. Click **Save** to apply the settings, and return to the panel.
3. To create a cascading hierarchy, drag the desired inputs/outputs from the left **Standard I/O List** to the group.

Note: In the cascading hierarchy, each input can only be used once while the same output can be used repeatedly.

Editing a Group:

To modify group settings, right-click a group, and select **View/Edit**. This dialog box appears.

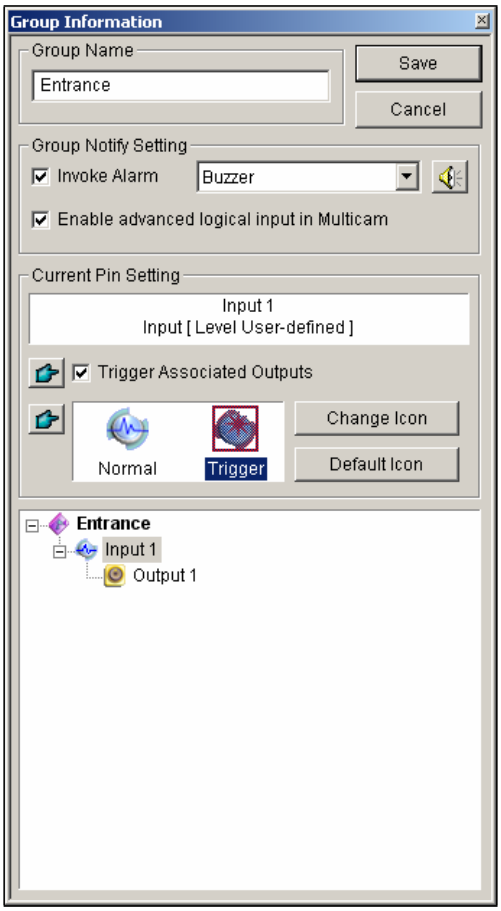


Figure 6-20

[Group Name] As described in Figure 6-19.

[Group Notify Setting] As described in Figure 6-19.

[Current Pin Setting] To enable this option, highlight an I/O device from the group list at the bottom.

④ **Trigger Associated Outputs:** Triggers outputs in cascade mode. Click the **Finger** button to apply the change to all I/O devices at the same group.

④ **Change Icon:** To enable this option, select one of two displayed icons: Normal or Trigger. Click the **Change Icon** button to change an icon. Click the **Finger** button to apply the change to all I/O devices at the same group.

Editing an I/O Device

In addition to editing groups, you can also edit the settings of individual I/O device. Right-click an I/O device, and select **Setting**. This dialog box appears.

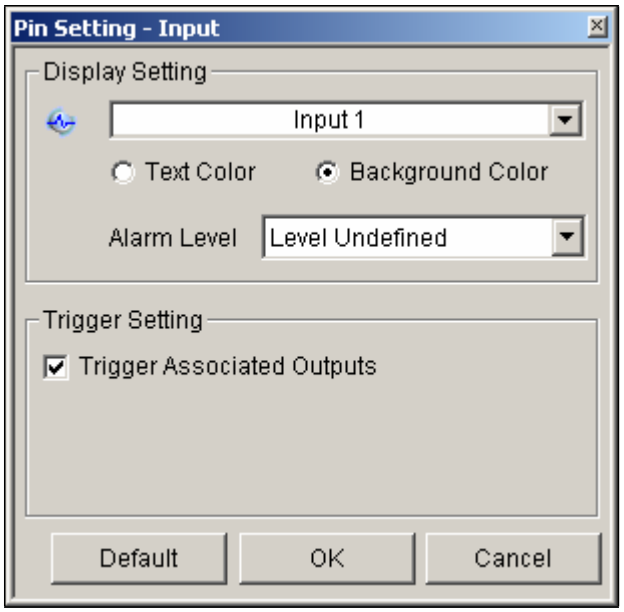


Figure 6-21

[Display Setting] You can define the nature of I/O devices by colors. Note that the setting only affects the **Detail** style of the Advanced I/O List (No. 4, Figure 6-17).

④ **Alarm Level:** Click the **Alarm Level** drop-down list, and select one of the six default colors: Fire, Smog, Vibration, Intruder, Motion and Emergency. For the Level Undefined option, select **Text Color** or **Background Color**, and then click the Input/Output drop-down list to change its color.

[Trigger Setting]

④ **Trigger Associated Outputs:** Triggers outputs in cascade mode (see *Creating a Group for Cascade Triggers* above).

6.6.3 Configuring the Advanced I/O Panel

On the panel toolbar, click the **Configure** button, and select **Panel Setting**. This dialog box appears.

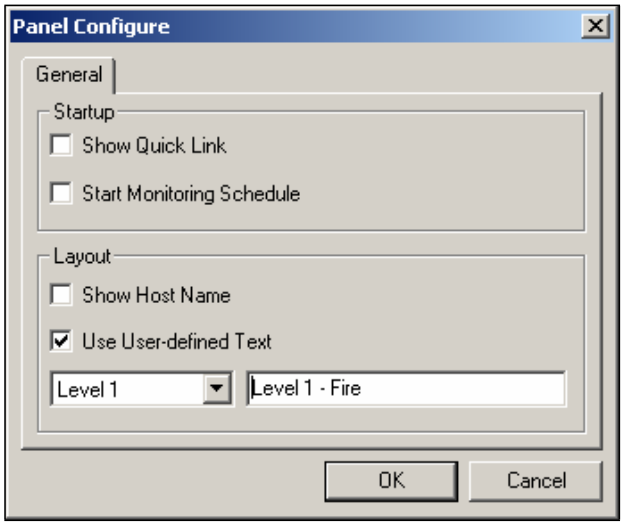


Figure 6-22

[Startup]

④ **Show Quick Link:** Opens the Quick Link window at panel startup.

④ **Start Schedule Monitoring:** Starts Mode Schedule at panel startup. For details, see *Setting up Mode Schedule* below.

[Layout]

④ **Show Host Name:** Displays the host name of each I/O device on the Advanced I/O List.

④ **Use User-defined Text:** Allows you to modify the text of Alarm Level (Figure 6-21).

6.6.4 Setting Up Mode Schedule

The Mode Schedule allows you to monitor different I/O cascade configurations at different time. For example, you may want I/O cascade triggers one way during business hours and another way for non-business hours. Modes can be switched automatically at a scheduled time.

Creating a Mode:

1. Click the Mode drop-down list (No. 7, Figure 6-17), and select **More Edit**. This dialog box appears.

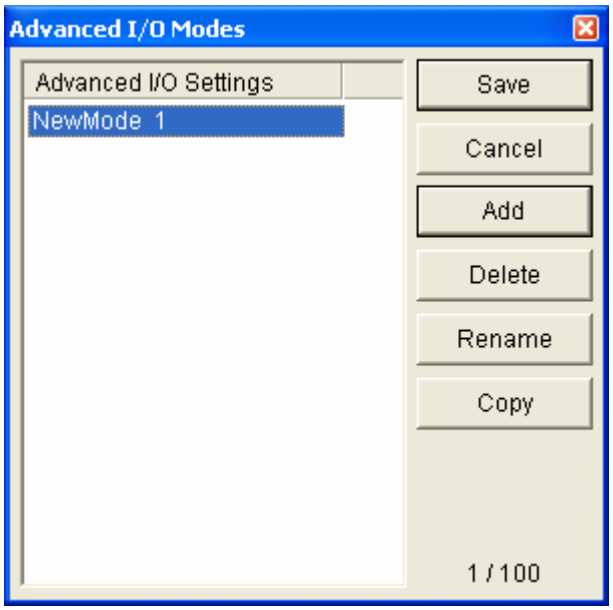


Figure 6-23

2. Click **Add**, and name the created mode. You can create up to 100 modes.
3. You can also apply the settings of the existed mode to the newly created mode. Click **Copy**, and select **from Default** to create a mode of default settings, or **select from selected Mode** to create a mode using the settings of the previously created mode.
4. Click **Save** to return to the panel.
5. Select the created mode from the **Mode** drop-down list, and create the groups in the Advanced I/O List. For details, see *Creating a Group for Cascade Triggers* earlier in this chapter.

Creating a Mode Schedule:

Define the times and days you like the panel to switch modes.

1. On the panel toolbar, click the **Configure** button, and select **Schedule Setting**. This dialog box appears.

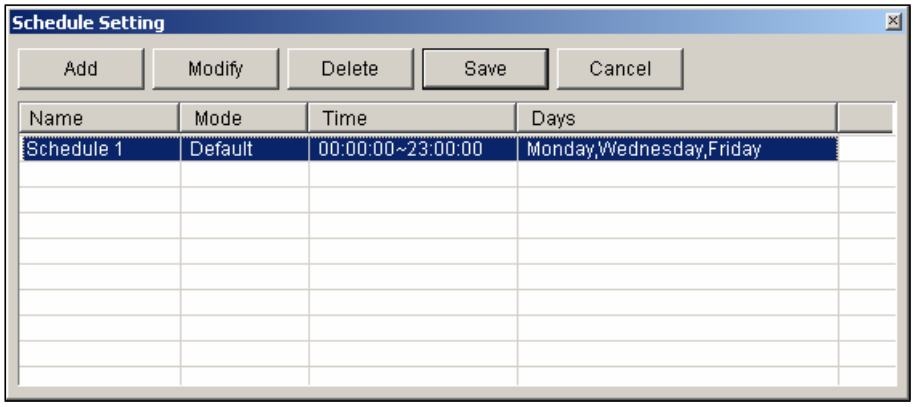


Figure 6-24

2. Click **Add** to create a schedule. This dialog box appears.

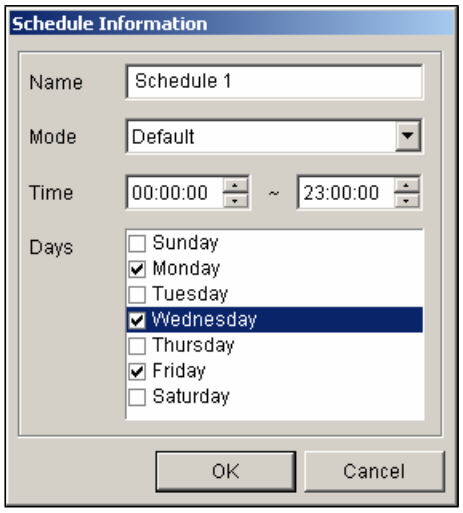


Figure 6-25

- ④ **Name:** Type a name for the schedule.
- ④ **Mode:** Select a mode from the drop-down list.
- ④ **Time:** Define a time period you want the mode to run.
- ④ **Days:** Check the day(s) you want the mode to run.

3. Click **OK** to apply the settings, and click **Save** to return to the panel.
4. To start the mode schedule, click the **Mode Schedule** button (No. 2, Figure 6-17), and then select **Mode Schedule Start**.

6.6.5 Quick Link

The Quick Link provides a quick access to triggered I/O devices. It is a separate window to display all group icons. The group icon flashes when any included I/O device is triggered. Clicking the flashing icon will bring you to the I/O location in the Advanced I/O List.

- To open the Quick Link window, click the **Toggle Quick Link** button. (No. 3, Figure 6-17).
- To set the Quick Link window at panel startup, see the **Show Quick Link** option in Figure 6-22.

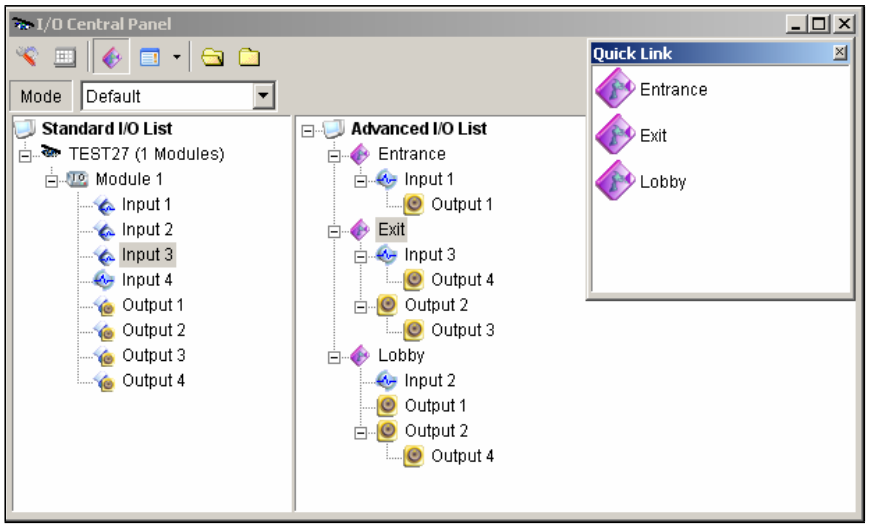


Figure 6-26

6.6.6 Forcing Output

To manually force an output, click one output, and select **Force Output**.

- In the Standard I/O List, you can force the output individually.
- In the Advanced I/O List, considering cascade triggers, you can only manually force the output at the top level, e.g. Figure 6-27. Other outputs at sub levels cannot be forced manually, e.g. Figure 6-28.

  However, if the output is not in a cascading hierarchy, you can definitely force it manually, e.g. Figure 6-29.

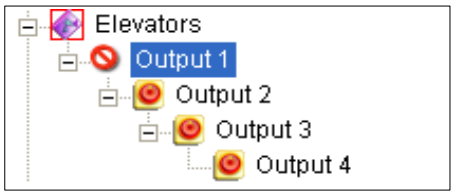


Figure 6-27

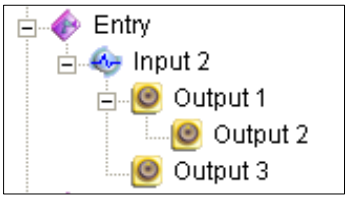


Figure 6-28

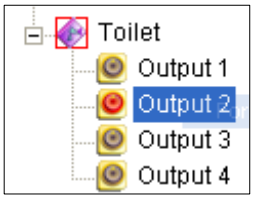


Figure 6-29

6.6.7 Editing Background Image

With the Background Image feature, you can import a floor plan to lay out the locations of triggered I/O devices. This feature works in the **Icon** style of the Advanced I/O List.

1. To switch to the Icon style, click the **Advanced I/O List Style** button (No. 4, Figure 6-17) and then select **Icon**.
2. Select a group in the Advanced I/O List. The I/O icons of this group will be displayed.
3. Right-click on the right screen, and select **Background Image** to import a graphic file.
4. Right-click on the right screen, and uncheck **Auto Arrange**. Now you can freely drag the I/O icons to the desired locations on the imported map.
5. To add images to another group, repeat the steps 2 to 4.

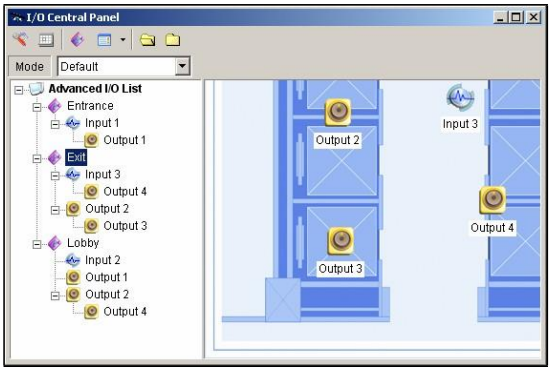


Figure 6-30

Note: Highlighting **Advanced I/O List** in the Advanced I/O List, you can import another image.

6.6.8 System-Wide Triggers

The System-Wide feature gives privileges to remote applications, such as Center V2 and VSM, to force the outputs in the Main System for cascade triggers.

For this example, the System-Wide feature is enabled in Output 1. When the VSM operator manually forces Output 1, Output 2, 3 and 4 will be triggered in a cascade series. If the System-Wide feature is disabled, the operator can only force Output 1 without cascade triggers.

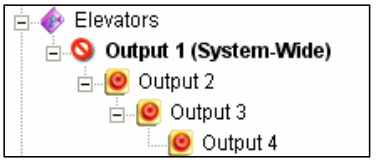


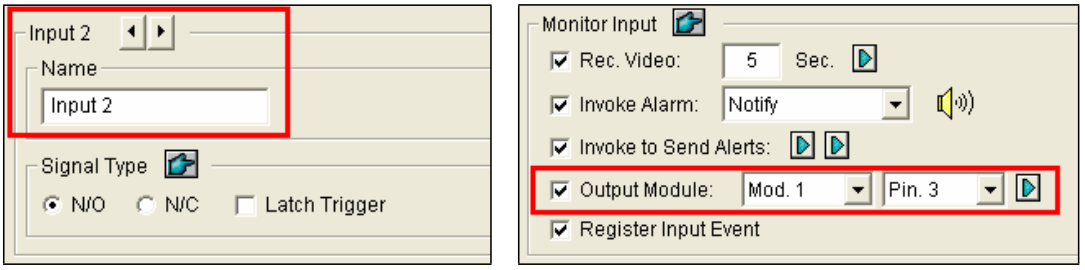
Figure 6-31

To enable this feature, right-click an output at the top level, and then select **System-Wide Output**.

6.6.9 The "Advanced Logical Input Status in Multicam" Option

If you already set a specific input to trigger a specific output in the Main System, you can decide whether to apply the simple input-trigger-output setting in the Advanced I/O Panel.

For example, you have set a simple access system in the Main System: Input 2 (card reader) triggers Output 3 (the door opens).



I/O Device Setup ***I/O Application Setting***

Figure 6-32

But to tighten security, you may set a group "Garage" in the Advanced I/O Panel. Both Input 1 (power switch) and Input 2 (card reader) should be activated together to trigger Output 1 (light), Output 2 (alarm) and Output 3 (the door opens) in a cascade series. Simply activating Input 2 (card reader) shouldn't cause any output triggers in the cascading hierarchy.

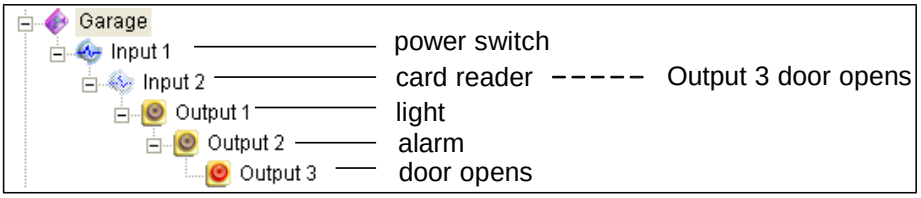


Figure 6-33

So now you have the options:

- At default, the simple input-trigger-output setting is applied at the Advance I/O Panel when **I/O monitoring** is activated. For this example, Input 2 will trigger Output 3.
- To only apply the cascade triggers set in the Advanced I/O Panel and ignore the simple input-trigger-output setting, enable **Use adv. Logical input result as input status** from the I/O icon on the main screen and **Enable advanced logical input in Multicam** from a certain group (see Figure 6-19) together.
- To switch to the simple input-trigger-output setting, just disable **Enable advanced logical input in Multicam**.

6.6.10 Managing a Group of I/O Devices

With groups of I/O devices set up on the I/O Advanced Panel, you can enable or disable these I/O devices by groups.

Enabling a Group

On the I/O Advanced Panel, right-click a desired group and select **Start Monitoring**. All input devices of this group are now enabled. When inputs are triggered, outputs will be activated in cascade mode.

Disabling a Group

On the I/O Advanced Panel, right-click a desired group and select **Stop Monitoring**. All input devices of this group are now disabled. No cascade triggers will occur.

Pausing the Triggered Inputs

This feature is designed for a group of outputs set to be Toggle mode. When inputs activate outputs in cascade triggers, right-click this group and select **Pause Monitoring**. The inputs of the group will be reset, but the outputs keep on alarming.

Note: With the **System-Wide Output** option (see *System-Wide Triggers* above) activated, you cannot use these three options to manage a group of I/O devices.

6.7 Visual Automation

The Visual Automation helps you automate any electronic device by triggering the connected output. You can intuitively click on the image of the electronic device to change its current state, e.g. light ON.

6.7.1 Setting Visual Automation

1. On the main screen, click the **Configure** button (No.14, Figure 1-2), point to **Accessories**, and select **Visual Automation Setting**. This dialog box appears.

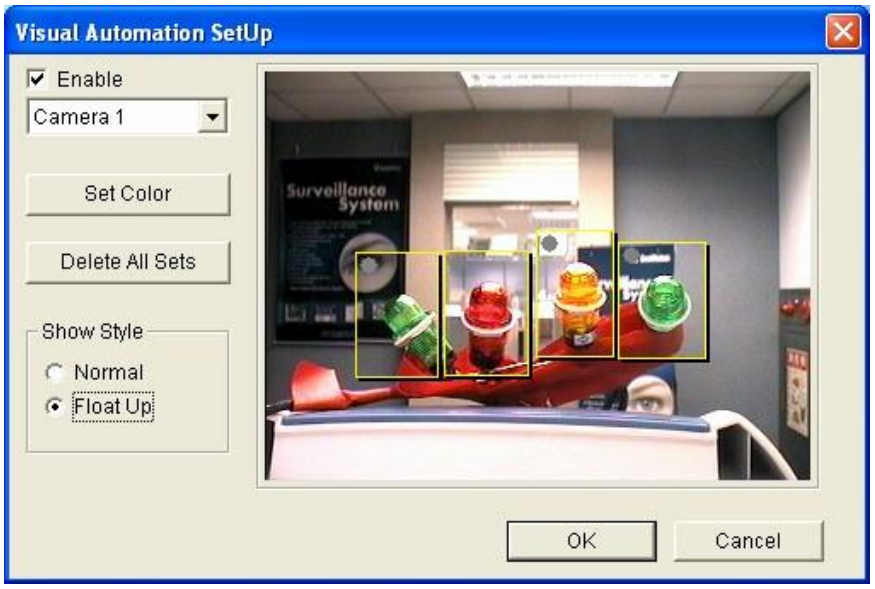


Figure 6-34

2. Select the desired camera from the drop-down list, and check **Enable**.
3. Drag the region on the image of the desired device. This dialog box appears.

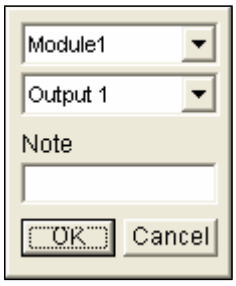


Figure 6-35

4. Select the connected module and output device. In the Note field, type a note to help you manage the device. Click **OK** to save the configurations.
5. To change the frame color of the set region, click the **Set Color** button.
6. To emboss the set region, check the **Float Up** option; or keep them flat by checking the **Normal** option.

6.7.2 Using Visual Automation

1. On the main screen, click the desired camera name (No. 2, Figure 1-2), and select **I/O Automation**. This window appears.

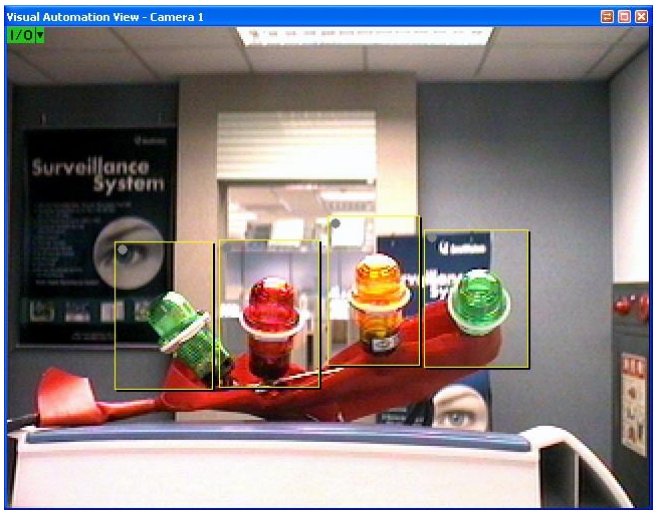


Figure 6-36

2. Click the set regions to force the connected output device.
3. To change the style of the set region, right-click the **I/O** icon to bring up these options:
   - ④ **Show All:** Displays all set regions.
   - ④ **Rect Float:** Embosses all set regions.
   - ④ **Set Color:** Changes the frame color of all set regions.

6.8 Virtual I/O Control

Through TCP/IP connection, the -System can remotely control the I/O devices connected from the -I/O Box of Ethernet module, -Wiegand Capture and IP devices.

On the main screen, click the **Configure** button (No.14, Figure 1-2), select **Accessories**, click **I/O Application** and select **Virtual I/O Setting**. This dialog box appears.

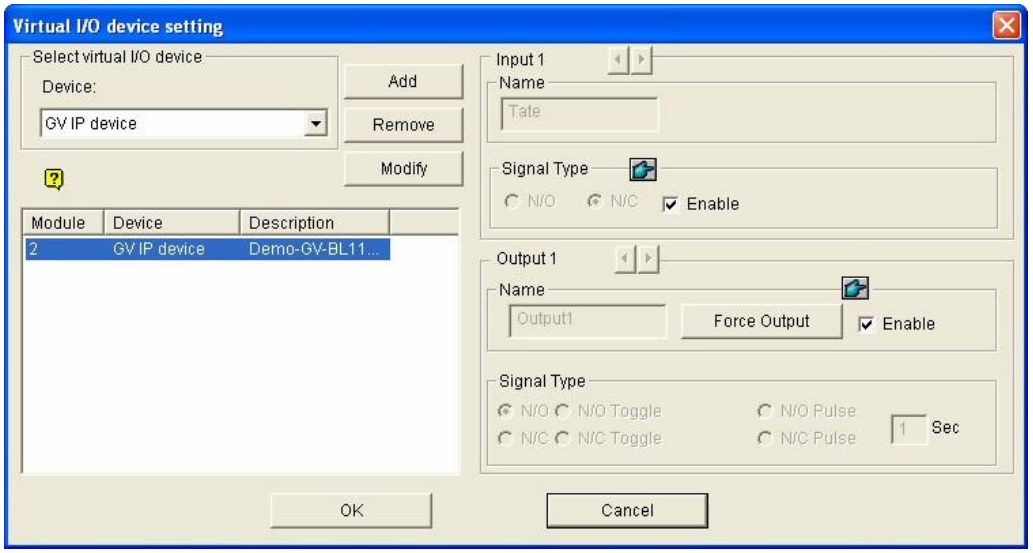


Figure 6-37

For details on the settings in the Virtual I/O Device Setting dialog box, see *I/O Device Setup* earlier in this chapter.

Note: The **Enable** option in the Signal Type section of the dialog box can turn on or off the I/O device of the added IP device.

6.8.1 Setting a Module

Up to 16 connected I/O devices can be combined to be one module for the -System to use. Note that I/O devices from -Video Server, -Compact DVR and -IP Camera can be combined to build a module. However, I/O devices of -Wiegand Capture or -I/O Box can only combine with those of another -Wiegand Capture or -I/O Box to set up a module.

1. Ensure the IP device, -Wiegand Capture or -I/O Box of Ethernet module has added to and recognized by the -System.
2. In the Virtual I/O Device Setting dialog box (Figure 6-37), select one device, e.g. **IP Device**, and click the **Add** button. This dialog box appears.

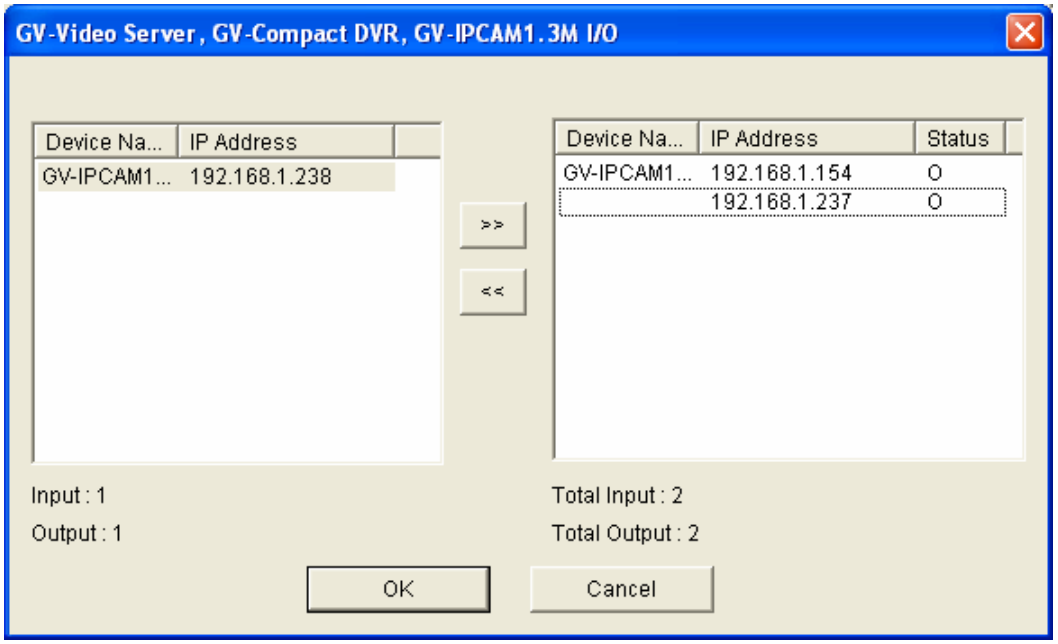


Figure 6-38

3. The connected devices appear on the IP address list. Select the desired devices and click the **[>>]** button to add their I/O devices to the Mapping list. The total number of added I/O devices is displayed at the bottom of the Mapping list. Click **OK**.
4. Select the added module from the list, and define the input status in the Monitor Input section. For details, see *[Input x]* in *I/O Device Setup* earlier in this chapter. Click **OK**.
5. On the main screen, click the **I/O** button (No. 7, Figure 1-2). This module is available from the selection list.

Chapter 7

Point-Of-Sale (POS) Application 351

7.1 Text-Mode POS Device 351

7.1.1 Windows-Based Direct POS Integration 351

7.1.2 Data Capture Box Integration 356

7.2 Graphic-Mode POS Device 357

7.2.1 Serial Port Connection 357

7.2.2 Network Connection 359

7.3 POS Device Setup 361

7.4 POS Data Overlay 363

7.5 POS Field Filter 365

7.6 Abnormal Transaction Alerts 367

7.6.1 Setting Alarm Frequency 368

7.7 Codepage Mapping 370

7.8 POS Data Search 371

7.9 POS Live View 372

7.9.1 The POS Live View Window 372

7.9.2 Setting Live View 373

7.10 POS Color Text 374

7.10.1 Setting POS Color Text 374

CHAPTER 7

Point-Of-Sale (POS) Application

A POS device can be integrated to the -System. You can view transactions as they happen overlaid on video channels. Transaction alerts can be configured, allowing instant notification of transaction events. Video searches can be performed based upon a specific transaction item or a period of time.

Before connecting a POS device to the -System, you need to know the printing mode of your POS device: Text Mode or Graphic Mode. If you are not sure about the printing mode of your POS device, refer to *The Printing Mode of POS System/Cash Register* at this link: http://www.Sting Alarm.com.tw/english/faq/POSflowchart/The_printing_mode_of_POS_system_cash_register.pdf

7.1 Text-Mode POS Device

7.1.1 Windows-Based Direct POS Integration

You can integrate a POS device to the -System without requiring a -Data Capture Box. The transaction data is directly transferred to the -System via a RS-232 serial cable or TCP/IP connection.

Before You Start

Before you start, note the specifications below for the integration:

- This integration supports Windows-based POS devices that can generate TXT, INI or JNL files and POS devices that are compatible with Internet or OPOS Printer Driver protocols.
- An appropriate dongle is required for the integration to work. The dongle options include 1, 2, 4, 8, 12 and 16 ports.
- For serial port connection, up to 4 POS devices can be connected to one -System. For TCP/IP connection, up to 16 POS devices can be connected to one -System.

Connection

Choose one of the following methods to connect the -System to a POS device.

RS-232 Connection

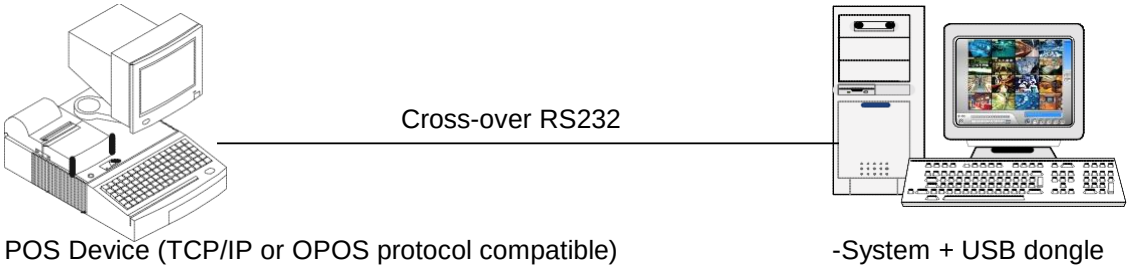


Figure 7-1

1. Using a cross-over RS-232 cable, connect the -System to the serial output of the POS device. The POS device needs to be capable of generating transaction files, or TCP/IP or OPOS protocol compatible.
2. Connect the USB dongle to the -System.

Network Connection

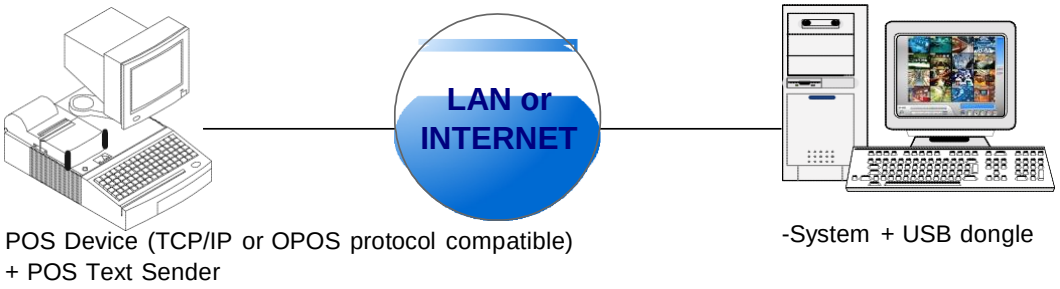


Figure 7-2

1. Connect the -System and POS device to the network. The POS device needs to be capable of generating transaction files, or TCP/IP or OPOS protocol compatible.
2. Configure a static IP address or domain name on the POS device. If the POS device uses a dynamic IP address, you should apply for a domain name from the DDNS service so that the -System can always access the POS device by the domain name.
3. Connect the USB dongle to the -System.

Note: Two kinds of DDNS programs are provided in the Software DVD: Dynamic DNS Service and Local DDNS Server. For details see *Chapter 11 Useful Utilities*.

Settings

At the POS device:

1. Insert the Software DVD to the POS computer. It runs automatically and a window appears.
2. Click **Install Sting Alarm Primary Applications**.
3. Select **-POS Text Sender [Only for Windows Based and Text Mode POS device]** and follow the on-screen instructions. This dialog box appears.

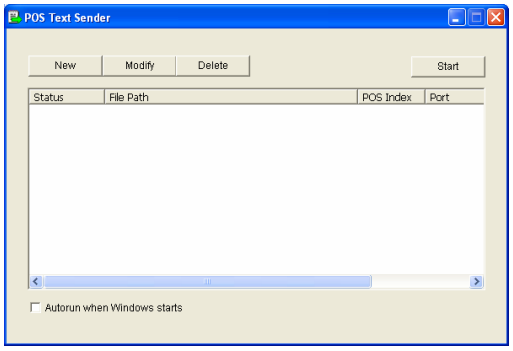


Figure 7-3

4. Click the **New** button. This dialog box appears.

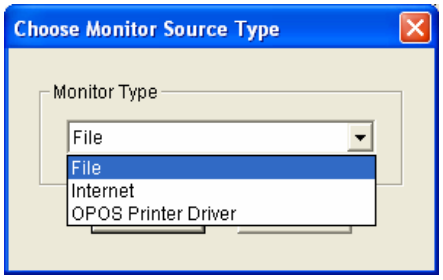


Figure 7-4

5. Select one of the following options.

   a. Select **File** if the POS device can generate TXT, INI or JNL files.

   b. Select **Internet** if the POS device is compatible with Internet protocol. Click **OK**. In the dialog box that appears, type the IP address of the POS device and the connection port. The default port value is 5111.

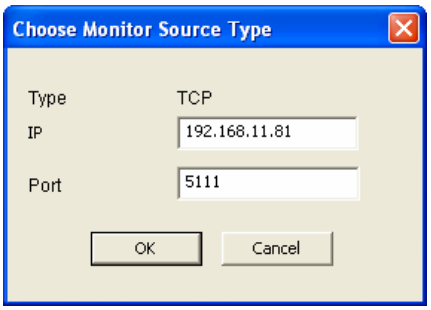


Figure 7-5

   c. Select **OPOS Printer Driver** if the POS device is compatible with OPOS protocol. Click **OK**. In the dialog box that appears, type the connection port. The default port value is 5111.

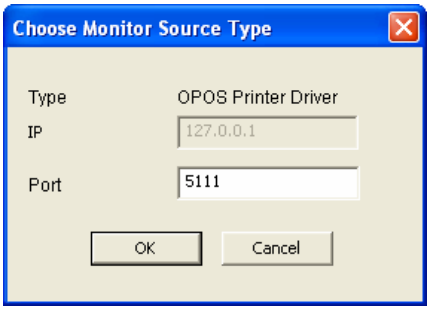


Figure 7-6

6. Click **OK**. This dialog box appears.

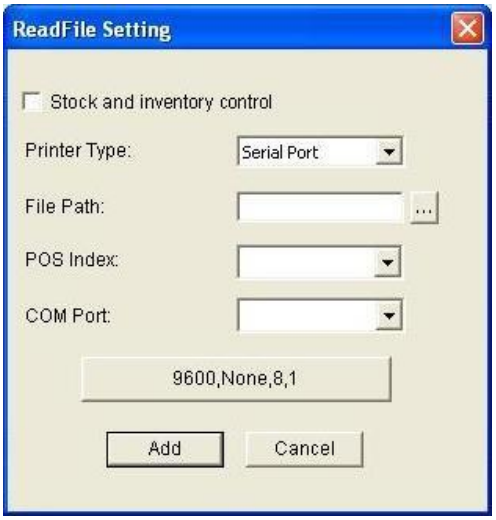


Figure 7-7

④ **Stock and inventory control:** Select to record identical transaction items as separate entries for receipts without receipt number and title. This function is useful for recording items entering or exiting a warehouse to keep track of the number of items currently in stock.

Note: This option is only available when you select **File** in the previous step. When connecting through **Internet** or **OPOS** protocols, identical transaction items are already recorded as separate entries for receipts without receipt number and title by default.

---

④ **Printer Type:** Select the type of the POS device: **Serial Port** or **TCP/IP Port**. Select Serial Port if the POS device is connecting to -System using a cross-over RS-232 cable. Select TCP/IP Port if the POS device is connecting through internet or OPOS protocols.

④ **File Path:** Locate the data file to be transferred to -System. This option is only available when you select **File** in the previous step.

④ **POS Index:** Number the POS device.

④ **COM Port:** Select the COM port that is used in connection with -System.

④ **The parameter/IP address button:**

For the serial type of POS device, click this button to configure Baud Rate, Data Bits, Parity and Stop Bits of the POS device.

For the TCP/IP type of POS device, click this button to configure Device Port and Password to match those of the -System. By default, the port value is 4000, and the password fields in both POS Data Sender and -System are left blank.

7. Click **Add** to apply the settings.
8. In the POS Text Sender dialog box, the POS device is added to the connection list. Click **Start** to start the connection. You can also minimize the dialog box to the notification area

.

At the -System:

It is required to insert an appropriate dongle to the -System for this integration to work. To set up a POS device in -System, see *POS Device Setup* later in this chapter.

Note: The maximum data size of each transaction to be transferred to a -System is 100 KB. When the data size of a transaction exceeds the limit, only the latest data will be transferred and displayed at the -System.

7.1.2 Data Capture Box Integration

For details on attaching the text-mode POS device to -System through -Data Capture Box, visit the related links below. POS System refers to that with a receipt printer attached internally, while Cash Register refers to that with a receipt printer attached externally.

To access	Visit
DB9 Interface POS System	http://www.Sting Alarm.com.tw/english/faq/POSflowchart/text/DB9_POS.pdf
DB25 Interface POS System	http://www.Sting Alarm.com.tw/english/faq/POSflowchart/text/DB25_POS.pdf
DB9 Interface Cash Register	http://www.Sting Alarm.com.tw/english/faq/POSflowchart/text/DB9_cash.pdf
DB25 Interface Cash Register	http://www.Sting Alarm.com.tw/english/faq/POSflowchart/text/DB25_cash.pdf

7.2 Graphic-Mode POS Device

You can integrate a graphic-mode POS device to the -System. The transaction data is directly transferred to the -System via a RS-232 serial cable or TCP/IP connection.

Before You Start

Before you start, note the specifications below for the integration:

- This integration only supports the Windows-based POS device.
- An appropriate dongle is required for the integration to work.
- For serial port connection, up to 4 POS devices can be connected to one -System. For TCP/IP connection, up to 16 POS devices can be connected to one -System.

7.2.1 Serial Port Connection

To attach the graphic-mode POS device, with the Windows operating system and serial output, to -System, follow these steps:

1. Connect the POS device as illustrated below.

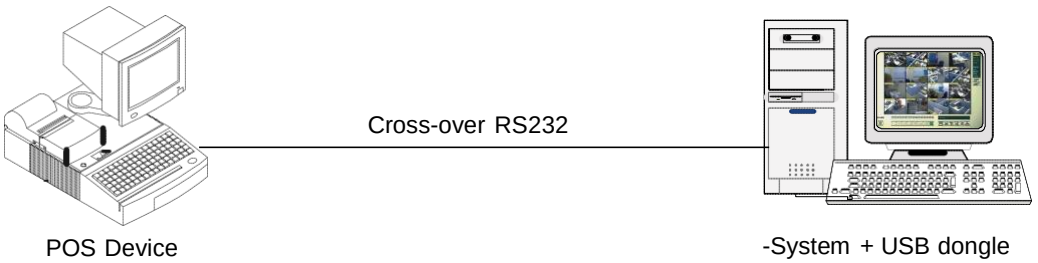


Figure 7-8

2. Insert the Software DVD to the POS device. It runs automatically, and a window appears.
3. Click **Install Sting Alarm Paid Software**.
4. Select **-POS Data Sender [Only for Graphic mode POS device],** and follow on-screen instructions to complete the installation.

5. Select **POS Data Sender** from Windows Start Menu. This dialog box appears.

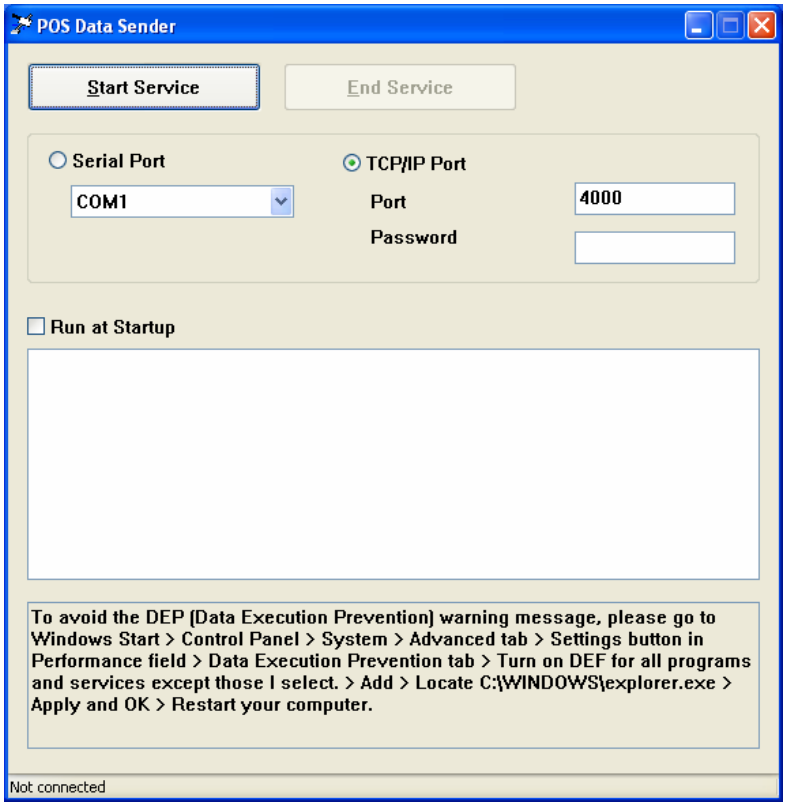

POS Data Sender
Start Service
End Service
Serial Port
COM1
TCP/IP Port
Port
4000
Password
Run at Startup
To avoid the DEP (Data Execution Prevention) warning message, please go to Windows Start > Control Panel > System > Advanced tab > Settings button in Performance field > Data Execution Prevention tab > Turn on DEF for all programs and services except those I select. > Add > Locate C:\WINDOWS\explorer.exe > Apply and OK > Restart your computer.
Not connected

Figure 7-9 *POS Data Sender*

6. Select **Serial Port** and select the **COM** port that the POS device is connected to.
7. Click **Start Service** to send graphic data to -System.

The -System must be configured and ready for this application. To set up the -System, see *POS Device Setup* later in this chapter.

7.2.2 Network Connection

1. Connect the -System and POS device to the network as illustrated below.

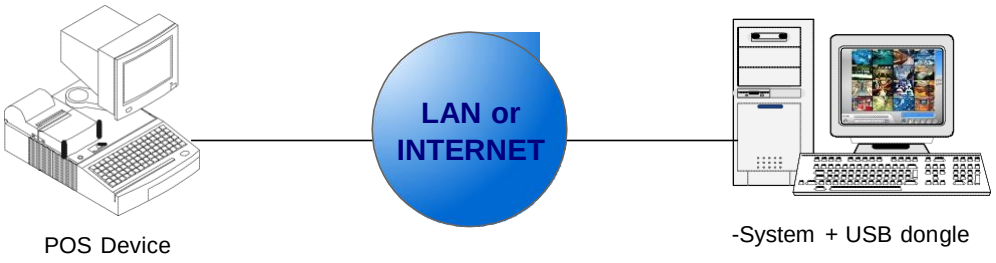
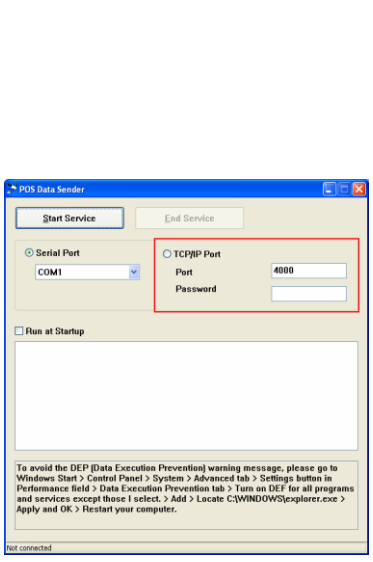
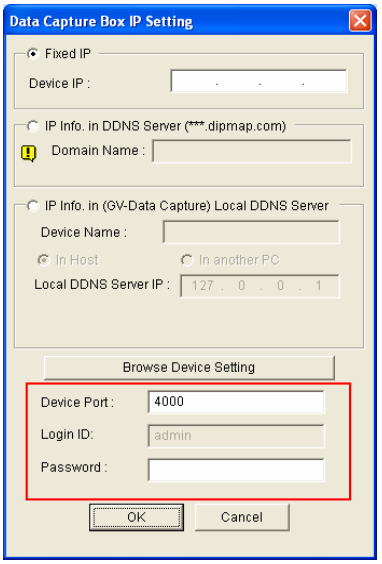


Figure 7-10

2. Insert the Software DVD to the POS device. It runs automatically, and a window appears.
3. Click **Install Sting Alarm Primary Applications**.
4. Select **-POS Data Sender [Only for Graphic Mode POS System]**, and follow on-screen instructions to complete the installation.
5. Select **POS Data Sender** from Windows Start Menu. The POS Data Sender dialog box appears.
6. Select **TCP/IP**.
7. Type Password or modify Port value to match those on the -System if necessary. By default, the port value is 4000, and the password fields in both POS Data Sender and -System are left blank. The first-time user can skip the step and follow the next step to test the connection.


POS Data Sender
Start Service
End Service
Serial Port
COM1
TCP/IP Port
Port
4000
Password
Run at Startup
To avoid the DEP (Data Execution Prevention) warning message, please go to Windows Start > Control Panel > System > Advanced tab > Settings button in Performance field > Data Execution Prevention tab > Turn on DEP for all programs and services except those I select. > Add > Locate C:\WINDOWS\explorer.exe > Apply and OK > Restart your computer.
Not connected

Settings on POS Data Sender



Settings on -System

Figure 7-11

8. Click **Start Service** to send graphic data to -System.

The -System must be configured and ready for this application. To set up the -System, see *POS Device Setup* later in this chapter.

7.3 POS Device Setup

To set up a POS device in -System, follow these steps:

1. On the main screen, click the **Configure** button (No. 14, Figure 1-2), select **Accessories**, click **POS Application Setting**, and select **POS Device Setup**. This dialog box appears.

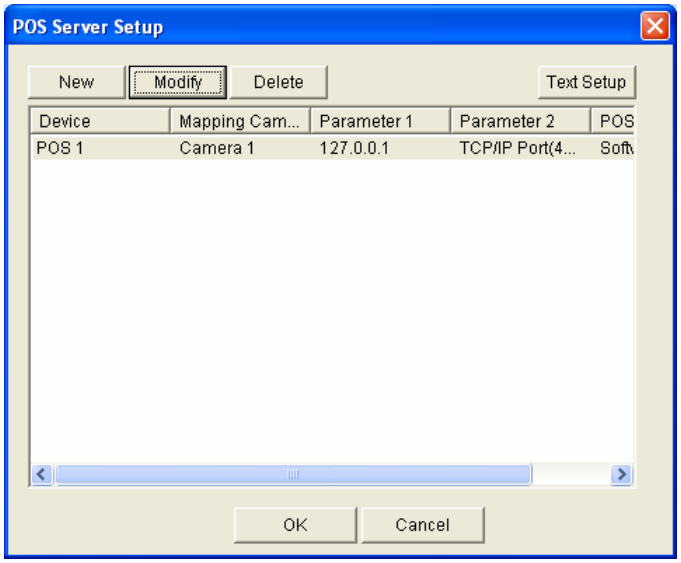


Figure 7-12 *POS Server Setup*

2. Click the **New** button. This dialog box appears.

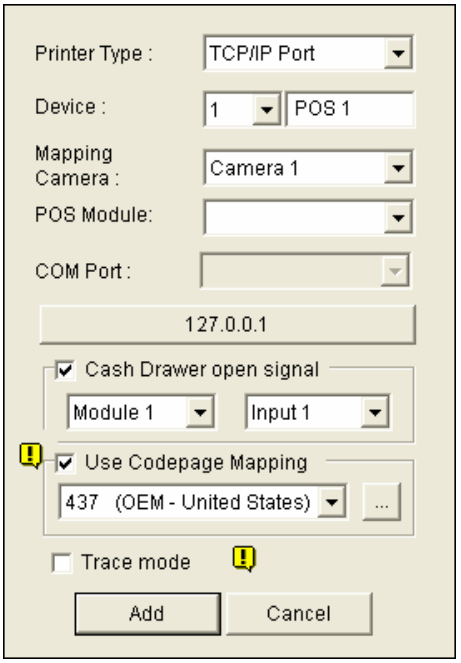


Figure 7-13 *POS system settings*

④ **Printer Type:** Select **Serial Port**, **Parallel Port** or **TCP/IP Port** that the POS device belongs to.

④ **Device:** Select the number of the POS device if multiple POS devices are connected, and rename it if necessary.

④ **Mapping Camera:** Assign the POS device to a camera screen.

④ **POS Module:** Select the printer attached to the POS device.

If it's not Epson, select **General** for other brands.

If the printing is the graphic mode, select **GraphMode**. For Graphic mode applications, see the *Graphic Mode POS Device* section above.

If the printing is the text mode and a -Data Capture Box is not used for integration, select **POS Text Sender**. For this application, see *Windows-Based Direct POS Integration* earlier in this chapter.

④ **COM Port:** Select the COM port that the POS device is connected to.

④ **The parameter/IP address button:**

For the serial type of POS device, click the button to configure Baud Rate, Data Bits, Parity, and Stop Bits of the POS device.

For the TCP/IP type of POS device, click the button to configure IP address, domain name or device name of the POS device.

④ **Cash Drawer Open Signal:** This option is only available when an input module is configured in the Main System. Assign the input module connected to the cash drawer. Every time when the cash drawer is opened, a signal will be sent to the Main System and recorded in System Log for later retrieval.

④ **Use Codepage Mapping:** This feature is to support special characters and symbols display. For details, see *Codepage Mapping* later in this chapter.

④ **Trace Mode:** Check this item only after getting the recommendation from our technical support staff.

3. After above settings, click **Add** to add the POS device to the Main System.

7.4 POS Data Overlay

Follow these steps to superimpose POS transaction data on the video.

1. Open the POS Server Setup window (Figure 7-12).
2. Click the **Text Setup** button to set text font and position of the data.

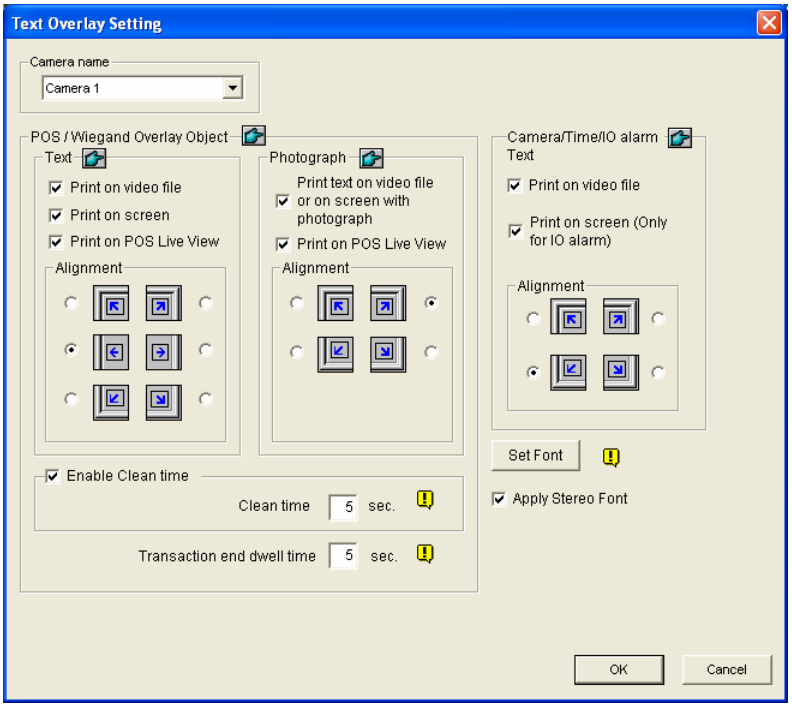


Figure 7-14 *Text Overlay Settings*

[Camera Name] Select a camera to be configured. After configuration, you can click the finger button at each section to apply the same settings to all cameras.

[Text]

④ **Print on video file:** Enable this option to display POS data on the recorded video file.

④ **Print on screen:** Enable this option to display POS data on the transaction scene.

④ **Print on POS Live View:** Enable this option to display POS data on the POS Live View window. See *POS Live View* later in this chapter.

④ **Alignment:** Select to set the position of text overlay on the screen.

[Photograph]

④ **Print text on video file or on screen with photograph:** Enable this option to overlay the photos with access text onto the live video or recorded file.

④ **Print on POS Live View:** Enable this option to display the photos on the POS Live View window. See *POS Live View* later in this chapter.

④ **Alignment:** Select to set the position of photo overlay on the screen.

[Enable clean time] When the option is enabled, after the specified time in seconds that if -System hasn't received the transaction data from your POS device, the already-displayed data will disappear from the camera screen, i.e. the cashier stops entering the transaction data.

④ **Transaction end dwell time:** Specify the amount of time in seconds that POS data stays on a camera screen before the next transaction.

[Camera/Time/IO Alarm Text]

④ **Print on video file:** Enable this option to display camera ID and location name on the recorded video file.

④ **Print on screen (Only for IO alarm):** Enable this option to display the name of triggered input device on the camera screen. For this function to work, it is required to map a camera to an input device, see *Overlaying Input Device Name onto Screen upon Input Trigger* in Chapter 6.

Note: Up to 5 input names can be stamped on each channel when inputs are triggered.

---

④ **Alignment:** Select how you want the camera information to be aligned on a camera screen.

[Set Font] Click the **Set Font** button to set up the font for POS and Camera/Time text. The option **Apply Stereo Font** makes texts stand out from the background by giving white-edge to the texts.

7.5 POS Field Filter

POS Field Filter allows you to create a column for a transaction item in System Log. It further filters the transaction conditions based on your criteria, and displays the results under the created column. To set up the function, follow these steps:

1. On the main screen, click the **Configure** button (No. 14, Figure 1-2), select **Accessories**, select **POS Application Setting**, and select **POS Field Filter Setup**. This dialog box appears.

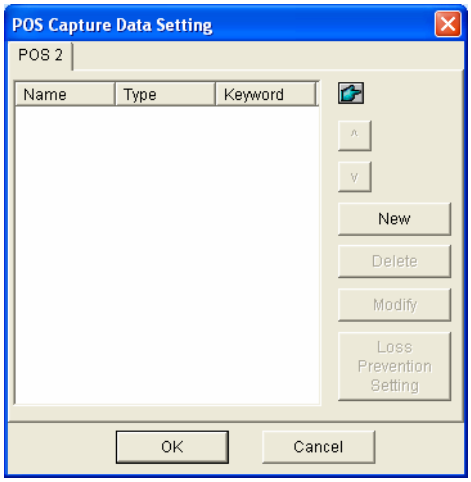


Figure 7-15 *POS Capture Data Setting*

2. Click the **New** button and select **Caption Data**. This dialog box appears.

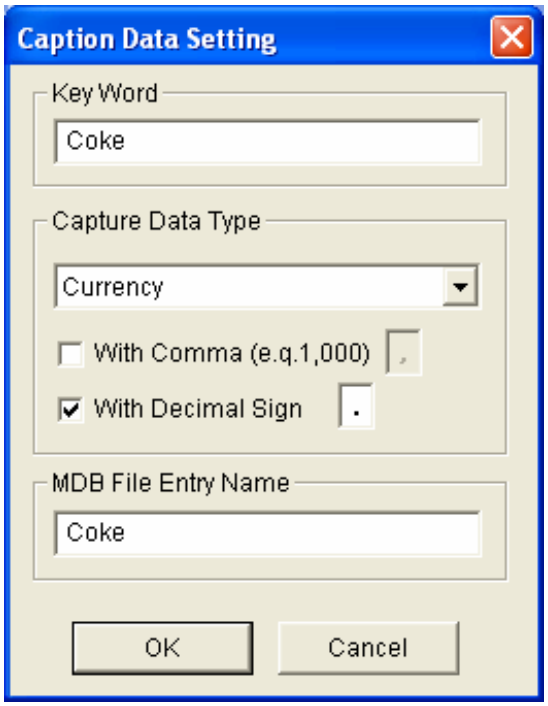


Figure 7-16 *Setting search criteria*

[Key Word] Enter a meaningful keyword that matches exactly one of transaction items/texts in the receipt. The field is case sensitive. Suppose we enter Coke, and every text matching to Coke will be screened out.

[Capture Data Type] Select the type of data followed by the specified transaction item/text: **Numeric**, **Currency** or **Alphabetic**. If the specified transaction item/text is followed by a price amount, select **Numeric** or **Currency**. If it is followed by alphabets, select **Alphabetic**.

④ **With Comma:** If there are commas in a price amount, select the option.

④ **With Decimal Sign:** If there are decimal signs in a price amount, select the option.

④ **With Space:** The option is only available when you select **Alphabetic**. If there is space among a series of characters, check the option.

[MDB File Entry Name] Enter a file name to store the data.

3. Click **OK** to apply the above settings.
4. In System Log, for this example, you can see the last column created for the transaction item Coke. The transactions matching the search criteria will be displayed under the created column.

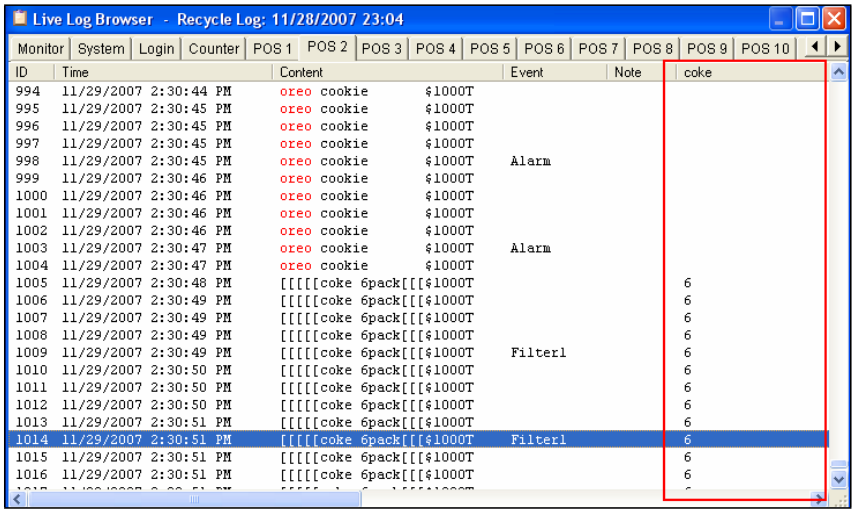


Figure 7-17 *A created column in System Log*

7.6 Abnormal Transaction Alerts

When an abnormal transaction of the specified transaction item occurs, this function can automatically activate the output device and send out assigned E-Mail/SMS/Pager alerts. To set up this function, follow these steps:

1. Follow the instructions in *POS Filed Filter* earlier in this chapter to set up a transaction item first.
2. In the POS Capture Data Setting dialog box (Figure 7-15), click the **Loss Prevention Setting** button. This dialog box appears.

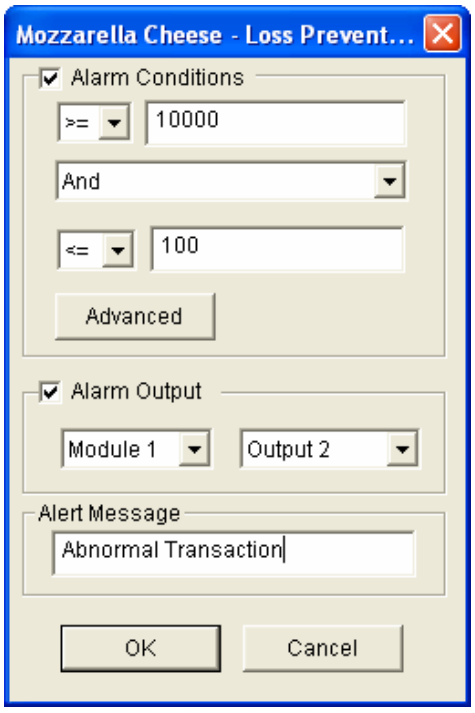


Figure 7-18 *Loss Prevention Setting*

[Alarm Conditions] Check this option and define the price range for an alarm condition. For this example, when the price amount in a transaction is *great than or equal to* (>=) 10000 and *less than or equal to* (<=) 100000, the assigned alarm will be activated.

[Alarm Output] Assign an installed output module for the application.

[Alert Message] Enter a desired alert message. To set up a notification type (E-Mail/Hotline/SMS), refer to *Send Alerts Approach* in Chapter 1.

7.6.1 Setting Alarm Frequency

To eliminate false alarms and increase monitoring efficiency, you can set up alarm frequency conditions.

In the Loss Prevention Setting dialog box (Figure 7-18), click **Advanced**. This dialog box appears.

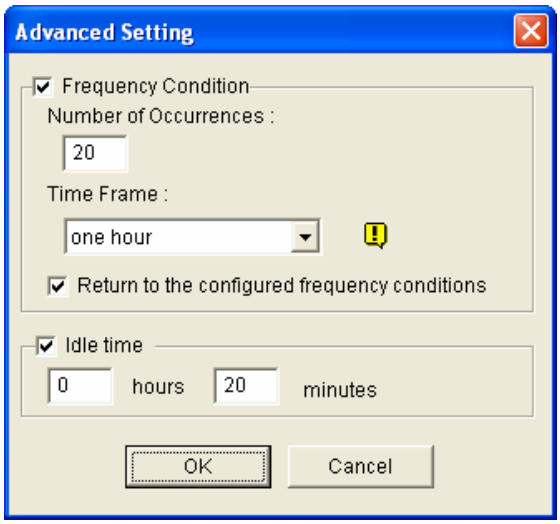


Figure 7-19

④ **Frequency Condition:** Enable to set up the number of event occurrences within a given time period to trigger the alarm.

- **Number of Occurrences:** Specify the number of event occurrences.
- **Time Frame:** Select one of the time periods: **one hour**, **12 hours**, **one day**, **one week** or **one month**.
- **Return to the configured frequency conditions:** After the alarm is triggered by the set frequency conditions, the system starts counting frequency again from zero. If this option was disabled and the frequency conditions have been met, the alarm will be triggered by every event.

④ **Idle time:** To avoid constantly triggered alarms, you can set the time interval between each event occurrence.

In System Log, the events that match the alarm frequency settings are marked with “Alarm.”

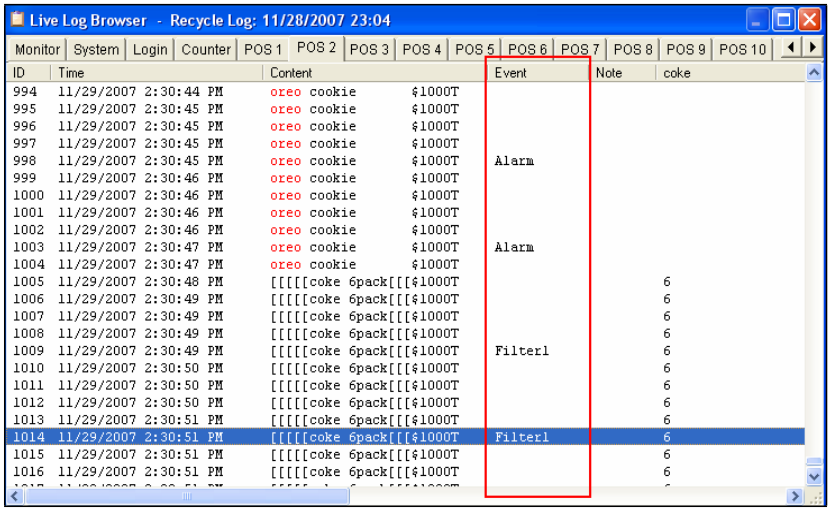


Figure 7-20

7.7 Codepage Mapping

This feature is to support special characters and symbols display. When your transaction text appears on the screen incorrectly, your POS device may use different character code from -System's. To change a character code, follow these steps:

1. In Figure 7-13, enable **Use Codepage Mapping**, and select a character code from the drop-down list.

Note: The codepage is related to "Script" in the **Set Font** option (Figure 7-14). When this option is disabled, it means there are no codepages matching your script setting.

---

2. To verify the character code you selected, click the **[…]** button to preview its codepage.

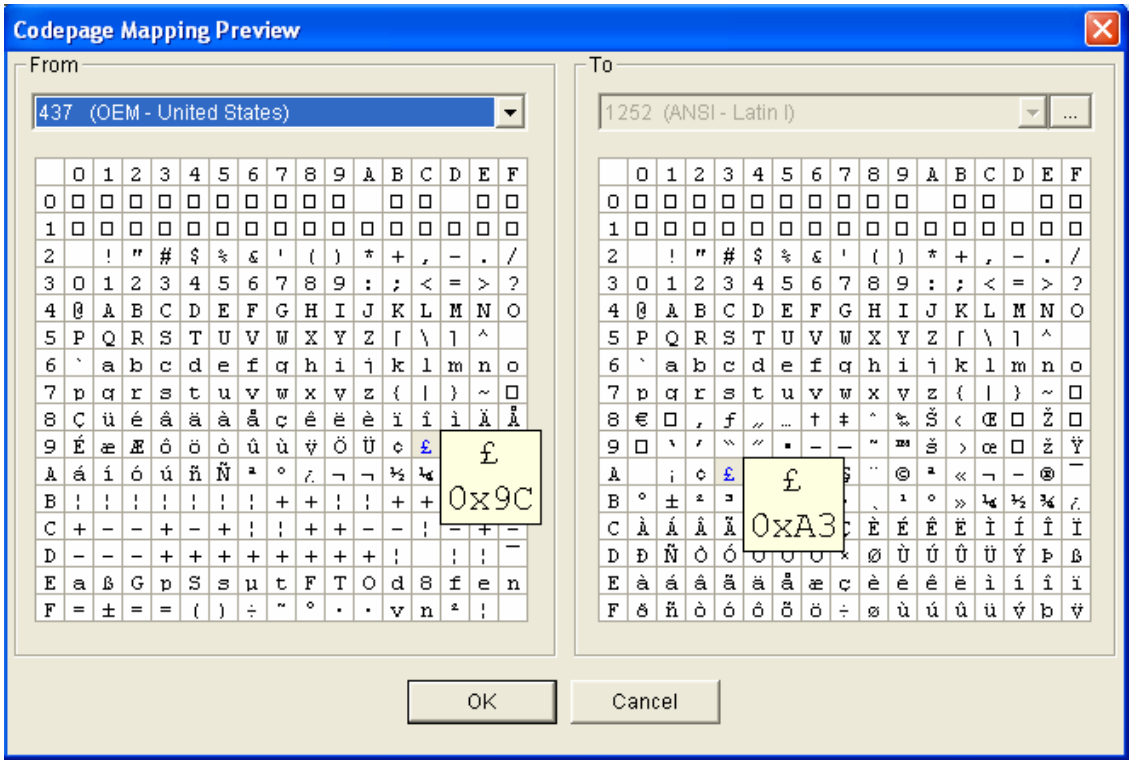


Figure 7-21 *Codepage Mapping Preview*

3. In the From field, locate and click one of the symbols or characters that couldn't display correctly. In this example, you can see its previous character code (From side: Ox9C) has been transferred to the default equivalent (To side: OxA3).

7.8 POS Data Search

You can locate any desired POS data and videos during a transaction. On the main screen, click the **ViewLog** button and then select **Search POS Data** to display the Quick Search window. When the Quick Search starts, the latest transaction video and data will always be displayed. For details on this feature, see *Quick Search* in Chapter 4.

Note: When IP cameras are installed with POS devices, note the following:

- In an Internet environment, the found POS data and images cannot match properly. Therefore, IP cameras are not recommended to be installed with POS devices in this condition.
- In a LAN environment, there will be image delay between found POS data and images. The delay is about 3 frames before or after the found data record.

7.9 POS Live View

The POS Live View can display transaction data in a separate window instead of overlaying data on the main screen. It features:

⌘ Fast access to transaction data without opening System Log.

⌘ The View is designed for high screen resolution of 1280 x 1024. When your monitor supports 1280 x 1024 and the main screen is set to 1024 x 768, you can juxtapose the main screen and the POS Live View.

7.9.1 The POS Live View Window

On the main screen, click the **ViewLog** button, and then select **POS Live View**.

Figure 7-22

The controls in the POS Live View Window:

No.	Name	Description
1	Previous Transaction	Goes to the previous transaction data.
2	Next Transaction	Goes to the next transaction data.
3	Freeze	Suspends the current transaction data display. Clicking this button again will restore to the live display.
4	Live View Menu	Accesses the settings of POS Live View.
5	Exit	Closes the POS Live View window.

7.9.2 Setting Live View

To change the display status on the POS Live View window, click the **Live View Menu** button (No.4, Figure 7-22) and select **Live View Setup**. This dialog box appears.

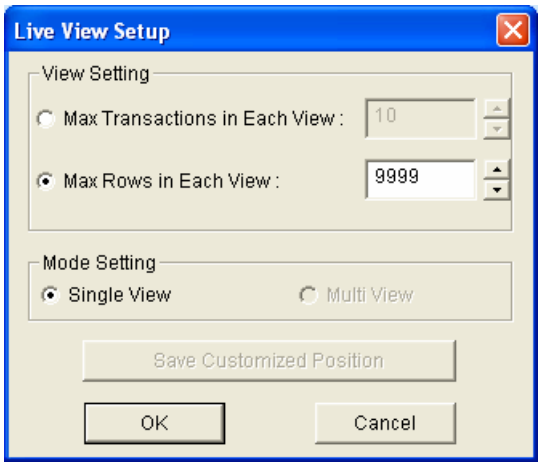


Figure 7-23

[View Setting]

④ **Max Transactions in Each View:** Enter the number of transactions you want to keep on the POS Live View window. For example, if you enter 99, there are always 99 transactions kept on the window. When the 100th transaction is entered, the oldest transaction data will be deleted and the max. transaction number remains to be 99.

④ **Max Rows in Each View:** Enter the number of transaction rows you want to keep on the POS Live View window, which includes any materials printed by the POS device, e.g. data and time.

[Mode Setting]

④ **Single View:** Displays only one POS Live View window on the screen.

④ **Multi View:** Displays multiple POS Live View windows on the screen.

④ **Save User Define Arrange Position:** Allows you to freely place the multiple windows on the screen.

To use this feature:

(1) Drag the windows to the desired places on the screen.

(2) Open the Live View Setup dialog box, and click this option. Click **Yes** to save your arrangement when this warning message appears: *Are you sure to save User Define Arrange Position?*

Whenever you want to place the POS Live View windows as your previous arrangement, click the **Live View Menu** button, point to **Arrange Views**, and select **Custom View**.

7.10 POS Color Text

You can use different colors and time periods to identify any desired transaction items. When the transaction item is identified, the feature can trigger the alarm and send out the alert message. The identification is recorded in the System Log for later retrieval as well.

For example, if the liquor is prohibited for sale in the midnight, a seller can use this feature to prevent from any unintentional sale.

7.10.1 Setting POS Color Text

1. On the main screen, click the **Configure** button (No. 14, Figure 1-2), point to **Accessories**, click **POS Application Setting**, and select **POS Field Filter Setup**. The POS Capture Data Setting dialog box (Figure 7-15) appears.
2. Click **New** and select **Color Keyword**. This dialog box appears.

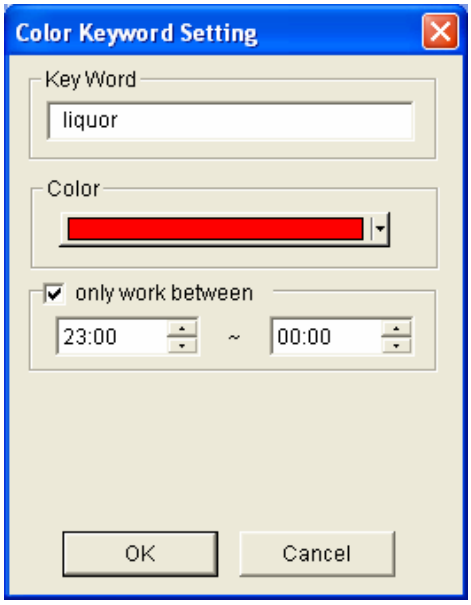


Figure 7-24

[Key Word] Type the text to be identified in the transaction data. The keyword setting is case sensitive.

[Color] Specify a color to identify the defined text.

[only work between] Specify the time period to identify the defined text in the transaction data.

3. To trigger an alarm when the defined text is detected during the transaction, click the **Loss Prevention Setting** button in the POS Capture Data Setting dialog box (Figure 7-15). This dialog box appears.

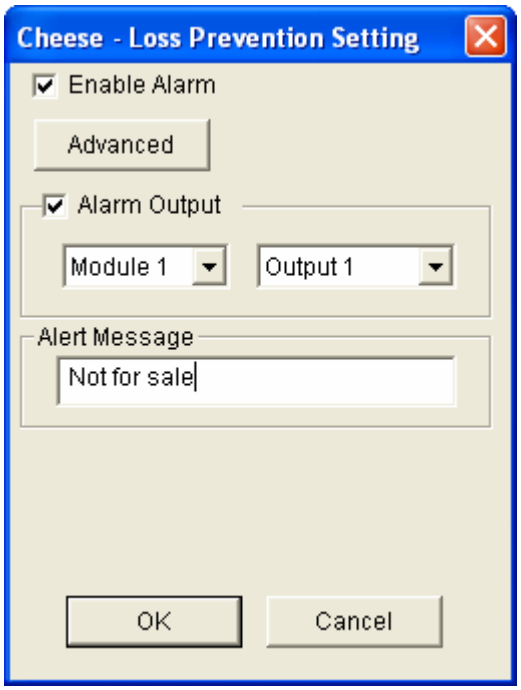


Figure 7-25

④ **Enable Alarm:** Check this item to enable the alarm when the identified text is detected. To set up alarm frequency conditions, click the **Advanced** button. For details, see *Setting Alarm Frequency* earlier in this chapter.

④ **Alarm Output:** Check this item and use the drop-down lists to select the connected module and output device.

④ **Alert Message:** Type the message for the E-mail or SMS alerts to be sent out when the alarm is triggered.

4. Click **OK** to save the above settings.

5. When the defined text is identified in the transaction data, the identification appears not only on the main screen but also on the POS Live View window. It is also recorded in the System Log.

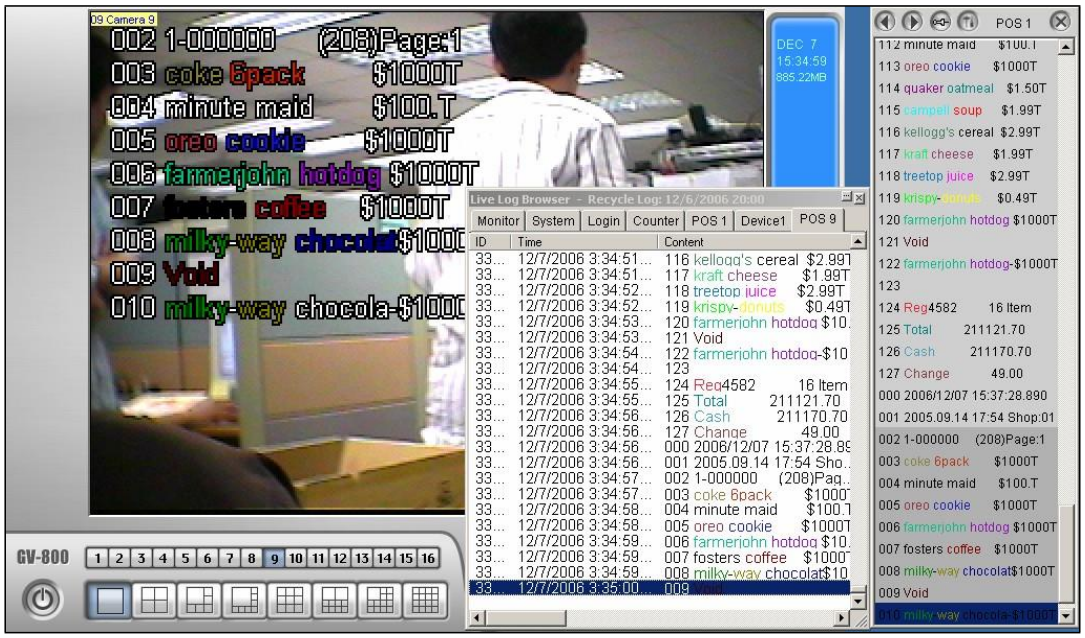


Figure 7-26

Note: You can set the maximum of 32 keywords for identification.

Chapter 8

Remote Viewing.....379

8.1 Remote Viewing Using a Web Browser 380

8.2 WebCam Server Settings 384

8.2.1 General Settings 384
8.2.2 Server Settings 385
8.2.3 Video Settings 386
8.2.4 SDK Settings 387
8.2.5 Audio Settings 388
8.2.6 JPG Settings 390
8.2.7 3GPP Settings 391
8.2.8 Mobile Settings 392
8.2.9 Multicast Settings 393
8.2.10 UPnP Settings 394
8.2.11 FTP Server Settings 397
8.2.12 Network Port Information 398

8.3 Single View Viewer 399

8.3.1 Control Panel 401
8.3.2 Server List 402
8.3.3 Video Recording 403
8.3.4 Alarm Notification 404
8.3.5 Video and Audio Configuration 405
8.3.6 Hardware-Compressed or Megapixel Stream 407
8.3.7 PTZ Control 408
8.3.8 Visual PTZ Control Panel 409
8.3.9 I/O Control 410
8.3.10 Visual Automation 411
8.3.11 Picture-in-Picture View 412
8.3.12 Picture-and-Picture View 413
8.3.13 Image Enhancement 414
8.3.14 Remote Configuration 415

8.4 2-Window Viewer 417

8.5 Multi-Window Viewer 418

8.6 Multi View Viewer 419
8.6.1 Installation of Multi View 419
8.6.2 Host List 423
8.6.3 Channel Status Information 424
8.6.4 Creation of a Host 425
8.6.5 Combination of Multiple Hosts into a Single Host 426
8.6.6 Video Recording 428
8.6.7 Camera Polling 429
8.6.8 Hardware-Compressed or Megapixel Stream 430
8.6.9 PTZ Control 431
8.6.10 Visual PTZ Control Panel 432
8.6.11 Output Control 433
8.6.12 Remote ViewLog 434
8.6.13 System Configuration 435
8.6.14 Camera Status 437
8.6.15 Host Information 438
8.6.16 Icon Image Change 439
8.7 Multicast and Audio Broadcast 440
8.7.1 Configuring Multicast and Broadcast Settings 440
8.7.2 Sending Audio Broadcast 442
8.7.3 Receiving Multicast and Audio Broadcast 443
8.8 JPEG Image Viewer 445
8.9 Remote Playback 446
8.10 Remote ViewLog 447
8.11 Event List Query 448
8.12 Download Center 450
8.13 Mobile Phone Applications 451
8.13.1 iPhone, iPod Touch, and iPad 452
8.13.2 Android Smartphones and Tablets 455
8.14 Web Browsers on Smartphones 459

CHAPTER

8

Remote Viewing

With Microsoft Internet Explorer, you can remotely view live video, download and play back video files, manage systems within the security network, control PTZ camera and I/O devices through the WebCam server.

The remote computer used to access live video must meet the following minimum requirements:

OS	32-bit	Windows XP / Vista / 7 / 8, Windows Server 2008
	64-bit	Windows 7 / 8, Windows Server 2008 / 2012
CPU		Pentium 4, 2.0 GHz
Memory	Windows XP	2 x 512 MB Dual Channels
	Windows Vista / 7 / 8 / Server 2008 / 2012	2 x 1 GB Dual Channels
Hard Disk		80 GB
Graphic Card		AGP or PCI-Express, 800 x 600 (1280 x 1024 recommended), 32-bit color AGP or PCI-Express, 1024 x 768, 32-bit color (for Multi View Viewer only)
Network		TCP/IP
Web Browser		IE 7.0 or later
DirectX		9.0c

With non-IE browsers, the below browsers are supported for remotely viewing live view, playing back videos and listing the event query only:

Google Chrome	21.0.1180.89m or earlier
Mozilla Firefox	15.0.1 or earlier
Apple Safari	5.1.7 or earlier

8.1 Remote Viewing Using a Web Browser

The -System is built in a WebCam server. Once the WebCam server is enabled, you can use Microsoft Internet Explorer, Google Chrome, Apple Safari, or Mozilla Firefox to remotely view and manage the surveillance images from the -System.

Note:

1. For Internet connection, the -System must have an IP address or domain name from ISP. If the IP address is dynamic, you may use the DDNS service to direct changing IP addresses to the -System. For the service, see *Dynamic DNS* in Chapter 11.
2. Make sure the remote PC is going to access the -System meets the minimum system requirements mentioned above.

---

1. To start the WebCam server on -System, click the **Network** button. The Server Setup dialog box appears. The first-time user can click **OK** without making any configuration to close the dialog box and start. When the WebCam server is started, “Web” and “CCS” signs appear on the main screen as illustrated below.

2. If there is a router or firewall installed on the server site of the -System, ensure the communication ports required by the WebCam Server is open: **80 (HTTP Port)**.

3. On any remote computer, open a Web browser and type the IP address or domain name of the -System. This dialog box appears.

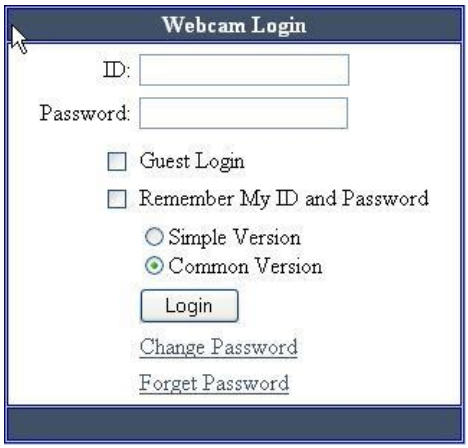


Figure 8-2

3. Type a user ID and a password created on the -System.
4. Click **Login**. When the connection is established, this Single View page appears.

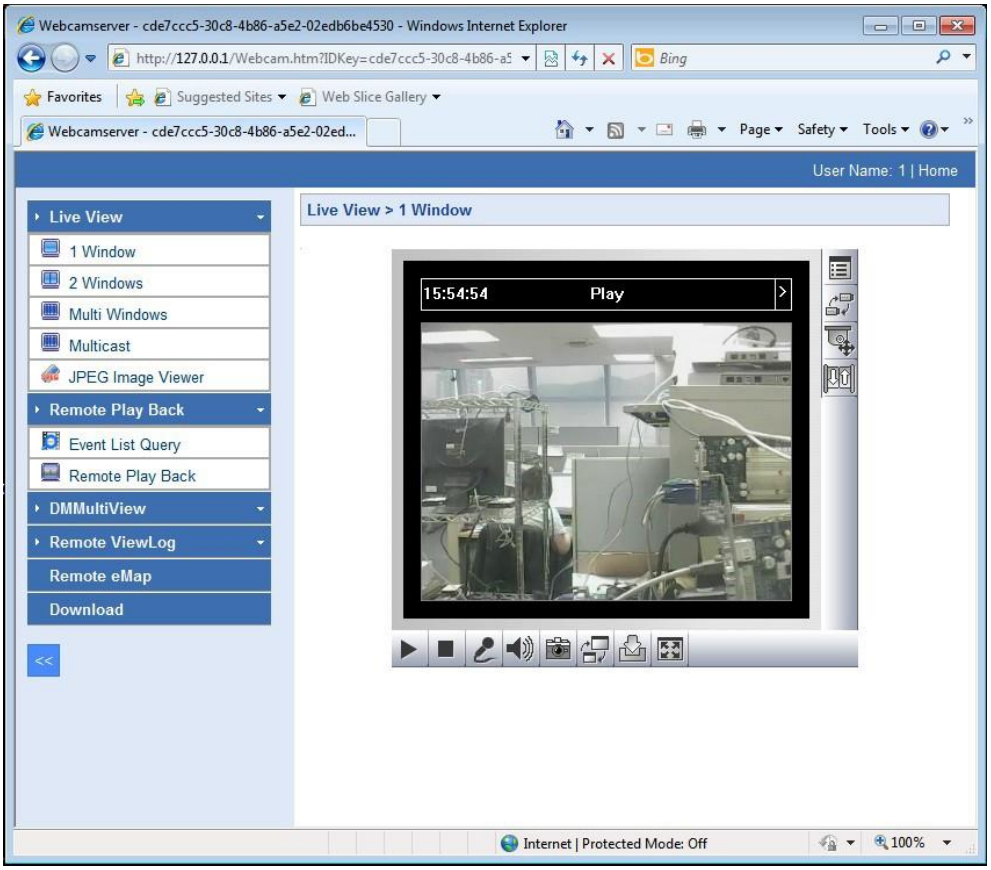


Figure 8-3 *Live View on IE Browser*

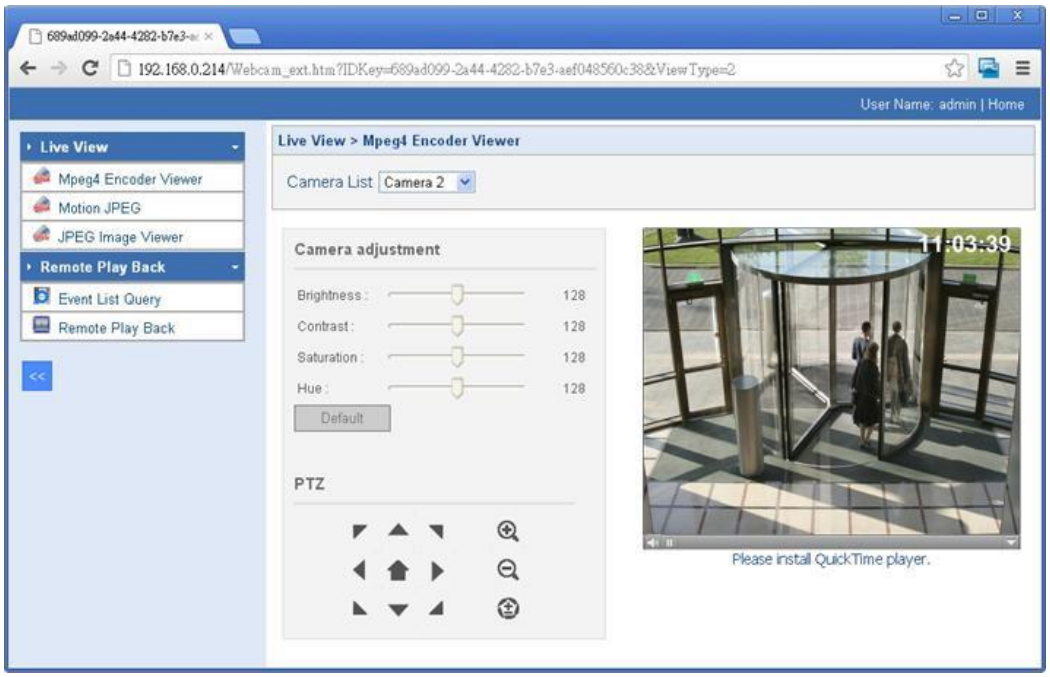


Figure 8-4 *Live View on Non-IE Browser*

The following WebCam server features will be introduced later in this chapter:

IE Browser's WebCam Server Features

Name	Description
Live View	Accesses different types of live view viewers. See *Single View Viewer*, *2-Window Viewer*, *Multi-Window Viewer, Multicast and Audio Broadcast,* and *JPEG Image Viewer* later in this chapter.
Remote Play Back	Accesses remote playback options. See *Event List Query* later in this chapter.
DMMultiView	Accesses the Multi View Viewer. See *Multi View Viewer* later in this chapter.
Remote ViewLog	Accesses the Remote ViewLog. See *Remote ViewLog* later in this chapter.
Remote E-Map	Accesses E-Maps remotely set up at the -System. See *E-Map Application* in Chapter 9.
Download	Accesses the Download Center. This function offers optional viewing programs to be downloaded to the local PC. See *Download Center* later in this chapter.
Home	Returns to the Login page.

Non-IE Browsers' WedCam Server Features

Name	Description
Live View	Accesses different types of live view viewers. For JPEG Image Viewer, see *JPEG Image Viewer* later in this chapter.
Remote Play Back	Accesses remote playback options. See *Event List Query* and *Remote Playback* later in this chapter.
Home	Returns to the Login page.

8.2 WebCam Server Settings

-System is built-in with a web sever. Click the **Network** button, and then select **WebCam Server** to display the following Server Setup dialog box. The Server Setup dialog box contains these tabs: (1) General, (2) Server, (3) Video, (4) SDK, (5) Audio, (6) JPG, (7) 3GPP, (8) Mobile and (9) Multicast.

8.2.1 General Settings

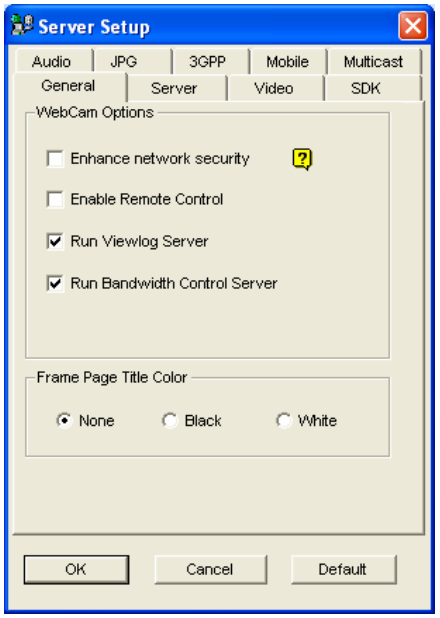


Figure 8-5

[WebCam Options]

④ **Enhance network security:** When this option is enabled, it is required to complete a word verification step every time when you log on to the WebCam server.

④ **Enable Remote Control:** Select this option to remotely configure the -System, PTZ cameras or I/O devices through the WebCam server.

④ **Run Viewlog Server:** Select this option to remotely play back video files through the WebCam server.

④ **Run Bandwidth Control Server:** Select this option to enable the **Bandwidth Control Server**. For details, see *Bandwidth Control Application* in Chapter 11.

[Frame Page Title Color] Select the color of date, time and camera stamps on the frame.

Note: When **Enhance network security** is enabled,

⌘ the users using earlier version than 8.0 cannot access WebCam applications any more, and

⌘ JPEG/3GPP/Mobile applications will be disabled.

8.2.2 Server Settings

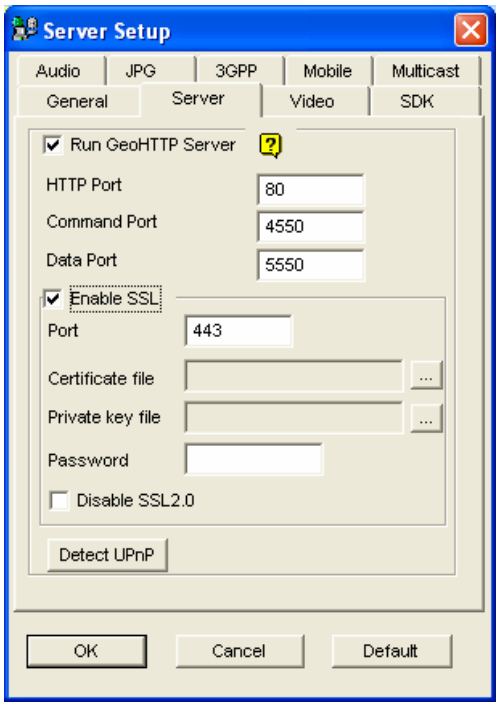


Figure 8-6

[Run GeoHTTP Server] Enable Geo-developed HTTP server or use your own HTTP server. Command Port is the port used to access WebCam, and Data Port is the port used to transfer data over Internet.

[Enable SSL] Enable the Secure Sockets Layer (SSL) protocol to ensure the security and privacy of Internet connection. To use your own generated Certificate and Private Key or ones verified by SSL authority, click the […] buttons and select the files stored at your computer. Note that the system will enable both SSL 2.0 and SSL 3.0 as its default; to disable SSL 2.0 protocol when using SSL 3.0, select **Disable SSL2.0.**

[Detect UPnP] For details, see *UPnP Settings* later in this chapter.

Note: If you want to enable SSL 3.0 on a computer running Windows Vista, it is required to upgrade your system to Service Pack 1 or Service Pack 2.

8.2.3 Video Settings

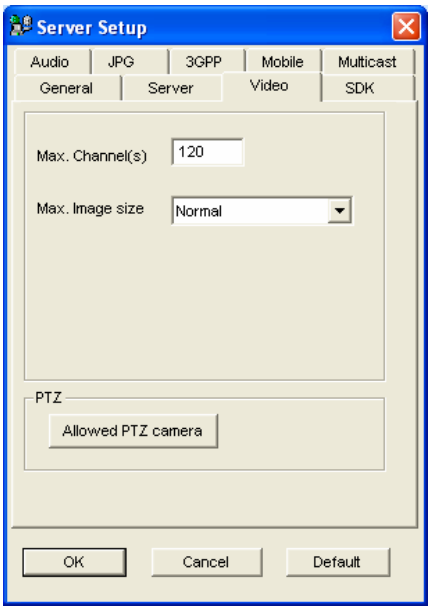


Figure 8-7

④ **Max. Channel(s):** Specify the number of channels allowed to access the WebCam server, with the upper limit of 200 channels.

④ **Max Image size:** Select a maximum resolution on the WebCam server. The default resolution on the WebCam is **Normal** (320 x 240).

- For DVR video source, if you want to view the image of **Middle** (640 x 480 (De-interlace), 704 x 480 (De-interlace)) or **Large** (640 x 480 or 704 x 480) size on the remote site, you also have to configure a corresponding Video Source at the -System. Click the **Configure** button on the main screen (No. 14, Figure 1-2), point to **A/V Setting**, and then select **Video Source**. In the Video Resolution field, select 640 x 480 or higher resolutions, and then click **OK** to apply.
- For IP video source, you may have larger size than DVR's. Besides normal, middle and large size, you can select **Actual Size** of that IP video. Refer to *Hardware-Compressed and Megapixel Stream* in *Single View Viewer* and *Multi View Viewer* later in this chapter.

④ **Allowed PTZ camera:** The option allows you to control selected PTZ cameras at a remote computer. Click the button and select the desired PTZ cameras to work on the WebCam server.

Note: To specify the time length allowed for a guest user to access the WebCam server, click the **Configure** button on the main screen, select **System Configure**, select **Password Setup**, and select **Local Account Edit**. On the WebCam tab, select the **Limit Connection Time** option and specify the time length. The time range is between 10 and 3600 seconds.

8.2.4 SDK Settings

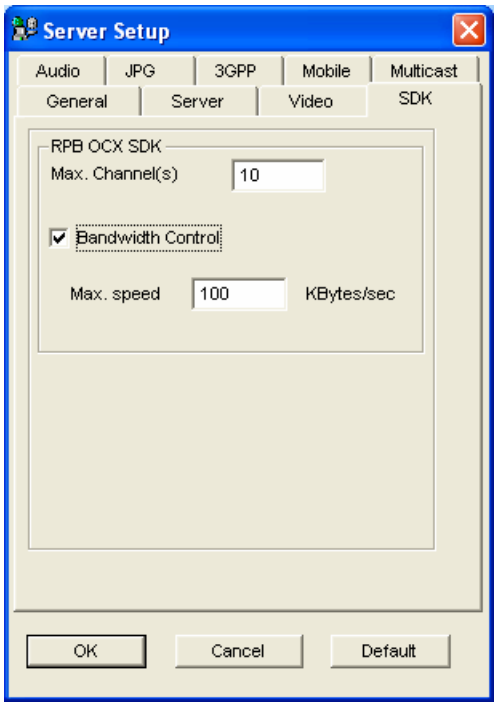


Figure 8-8

This feature is only used for SDK users to prevent overloading on slower networks.

④ **Max. Channel(s):** Specify the number of channels allowed to be downloaded to a client PC.

④ **Bandwidth Control:** Enable and specify the rate of data to be transferred over network. The option effectively controls the bandwidth being used by the WebCam server.

8.2.5 Audio Settings

Connecting Audio Devices

Through the WebCam server, you can access live audio at a remote site and talk to the server site. This feature is useful when the remote site requires speaking to the personnel at the server site in case of emergency. Before using this feature, make sure all the necessary hardware are in place:

1. To record audio, connect microphones to the audio inputs on the -Video Capture Card. For details, refer to the *-DVR and Accessories Installation Guide* on the Software DVD.
2. Make sure your sound card is already inside the computer. Connect a multimedia speaker to the audio output of your computer's sound card. This is for receiving audio from the remote site.
3. Connect a desktop microphone to the input of the audio extension card (or cable line). This is for sending audio to the remote site.

Audio Setup

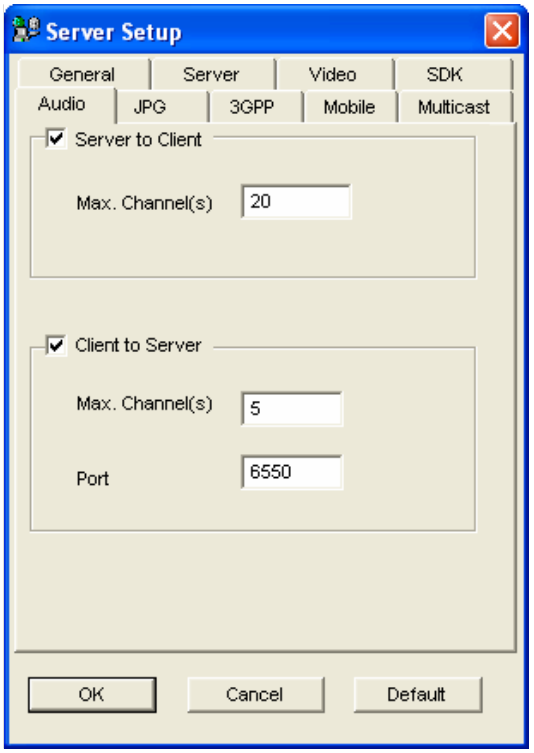


Figure 8-9

[Server to Client] Allows a remote computer to access live audio from the server site of the -System.

④ **Max. Channel(s):** Enter the number of remote computers allowed to access live audio, with the upper limit of 40 PCs.

[Client to Server] Allows a remote computer to speak to the server site of the -System.

④ **Max. Channel(s):** Enter the number of remote computers allowed to speak to the server site, with the upper limit of 20 computers.

④ **Port:** The default audio port is 6550.

8.2.6 JPG Settings

These settings allow you to send JPEG or GIF files over Internet.

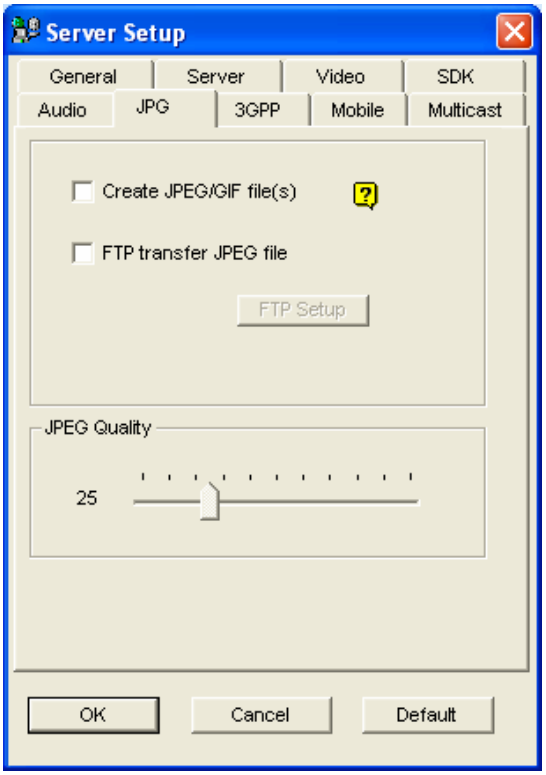


Figure 8-10

④ **Create JPEG/GIF file(s):** Allows you to view the JPEG/GIF images remotely. You can use the JPEG Image Viewer feature of the WebCam server to access the JPEG images over Internet. Enabling this function also allows you to use mobile applications i-Mode, -Remote View, -iView and -AView to access the JPEG images on your mobile phone. After the feature is enabled, use the slider to adjust JPEG image quality. The bigger the number (sliding it towards right), the better the image quality and the bigger image file size.

④ **FTP Transfer JPEG file:** Downloads JPEG images from the FTP server. For details, see *FTP Server Settings* later in this chapter.

8.2.7 3GPP Settings

These settings allow you to stream video and audio on 3G-enabled mobile phones.

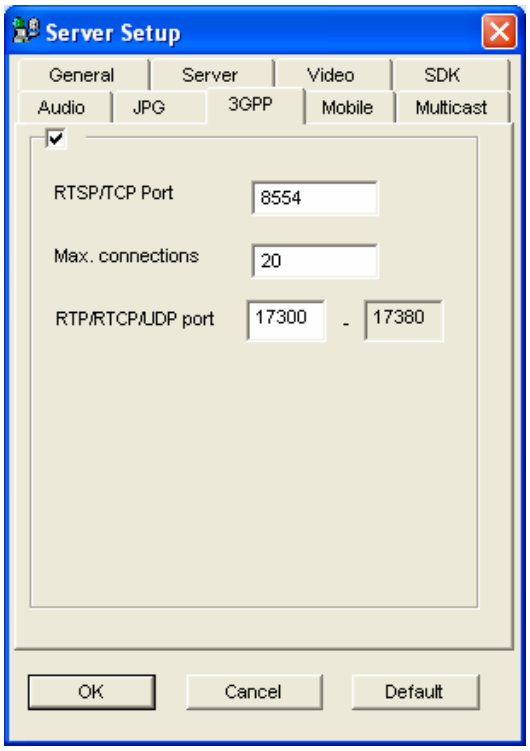


Figure 8-11

④ **RTSP/TCP Port:** The default communication port is 8554.

④ **Max. Connections:** Specify the number of users that can connect to this server. Set the number to be between 1 and 100.

④ **RTP/RTCP/UDP Port:** The number of ports is limited to 80 in order to enhance the security of the WebCam server during the connection with the 3G-enabled mobile phones. The default range of ports is 17300 to 17380.

Note: To enable 3G services on your mobile phone, consult your network operator.

8.2.8 Mobile Settings

These settings allow you to perform mobile phone applications. For details, see *Mobile Phone Applications* later in this chapter.

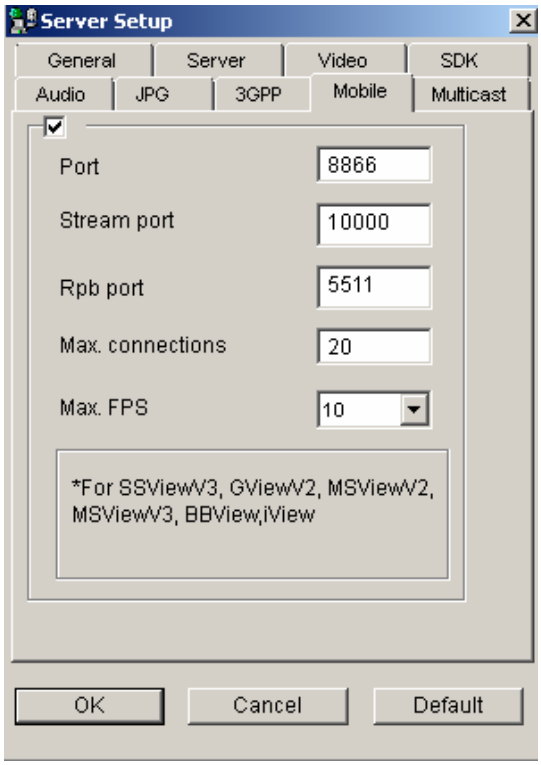


Figure 8-12

④ **Port:** The default communication port is 8866.

④ **RPB port:** This port is used for remote playback feature. The default value is 5511. For this feature to work, the **Run ViewLog Server** option (Figure 8-5) must be selected too.

④ **Max. connection:** Specify the number of users that can connect to this server. Set the number between 1 and 20.

8.2.9 Multicast Settings

These settings allow you to perform multicast and audio broadcast functions. For details, see *Multicast and Audio Broadcast* later in this chapter.

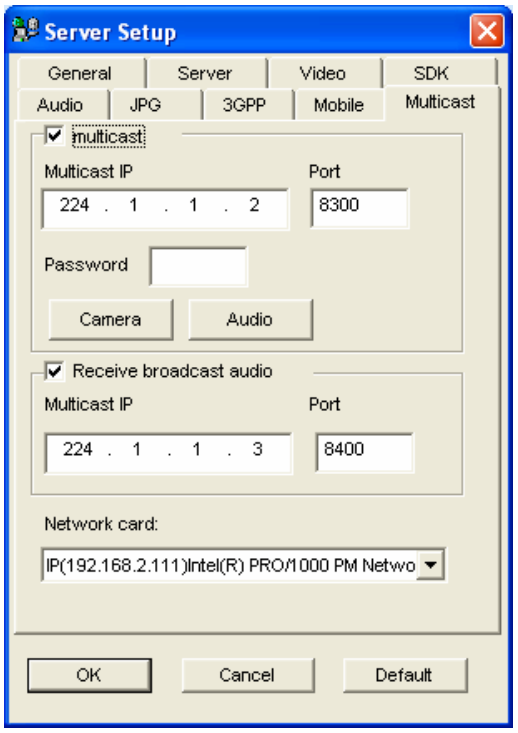


Figure 8-13

④ **Multicast:** By default the IP address is 224.1.1.2, and port number is 8300 to send the video and audio stream. Optionally, you can specify a **Password** for hosts to activate multicast. Click the **Camera** and **Audio** buttons to select which camera and audio are accessible through multicast.

④ **Receive Broadcast Audio:** By default the IP address is 224.1.1.3, and port number is 8400 to receive audio broadcasting.

④ **Network Card:** Select another network card, if available, to run the Multicast service on a different network. Since the Multicast service can take a lot of bandwidth when enabled, separating it from the main network is advised whenever possible.

8.2.10 UPnP Settings

WebCam Server supports UPnP technology (Universal Plug and Play) to allow automatic port configuration to your router.

In order for UPnP to be enabled, the following requirements must be met:

⌘ Windows XP Service Pack 2 or above

⌘ Windows XP must be configured to use UPnP (see below)

⌘ UPnP must be enabled on your router (consult your router's documentation)

Enabling UPnP in Windows XP

1. Go to Windows Start, click **Start** button, select **Settings**, and select **Network Connections**. This window appears.

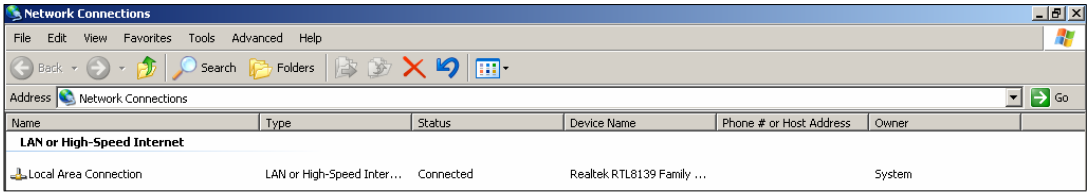

Network Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network Connections
Go
Name Type Status Device Name Phone # or Host Address Owner
LAN or High-Speed Internet
Local Area Connection LAN or High-Speed Inter... Connected Realtek RTL8139 Family ... System

Figure 8-14

2. Right-click one **Local Area Connection**, select **Properties**, and click the **Advanced** tab. This dialog box appears.

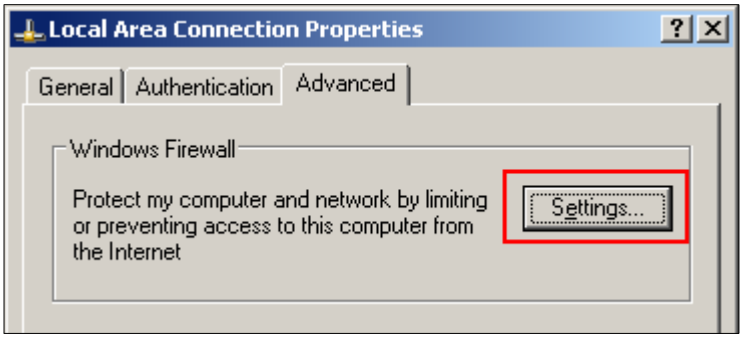


Figure 8-15

3. Click the **Settings** tab, and click **Exceptions** tab. This dialog box appears.

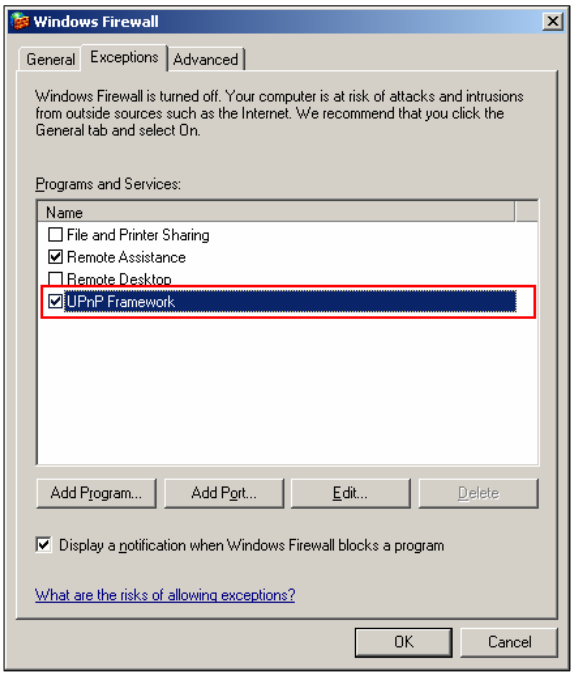


Figure 8-16

4. Select **UPnP Framework**, and click **OK**.

Enabling UPnP on the WebCam Server

1. On the main screen, click the **Network** button (No. 11, Figure 1-2), select **WebCam Server**, and click the **Server** tab. The Server Setup dialog box (Figure 8-6) appears.
2. Click **Detect UPnP**. This dialog box appears.

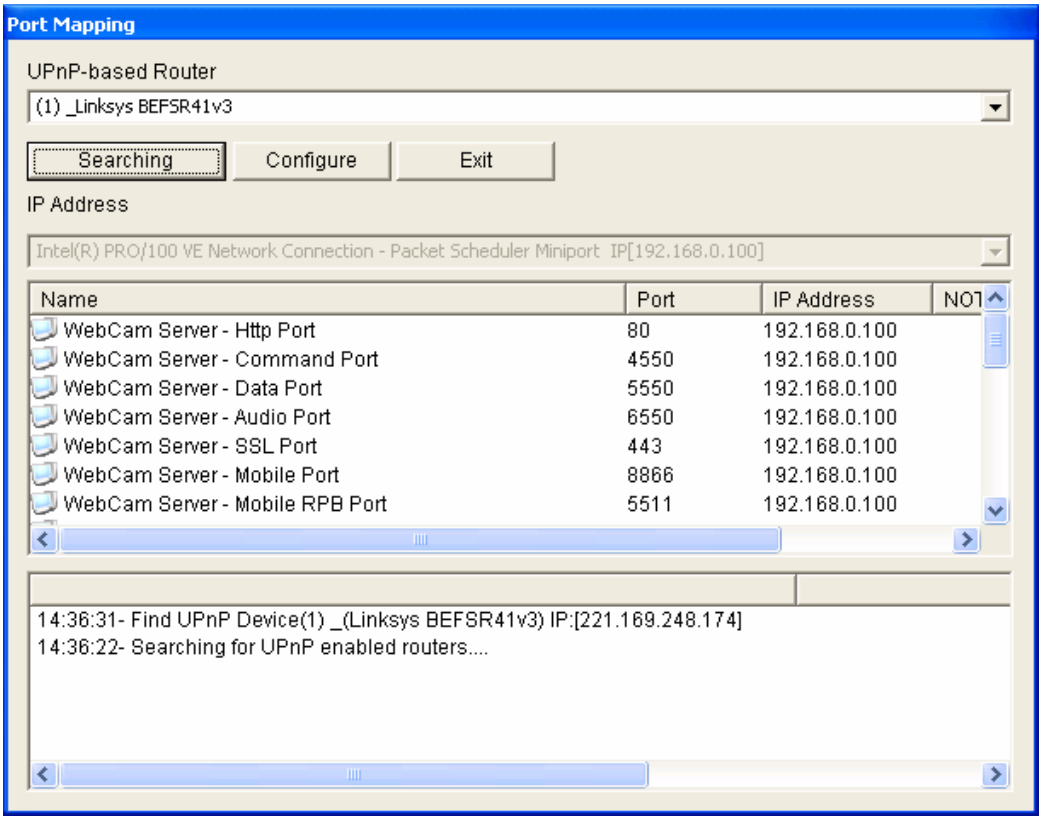

Port Mapping
UPnP-based Router
(1) _Linksys BEFSR41v3
Searching
Configure
Exit
IP Address
Intel(R) PRO/100 VE Network Connection - Packet Scheduler Miniport IP[192.168.0.100]
Name
Port
IP Address
WebCam Server - Http Port 80 192.168.0.100
WebCam Server - Command Port 4550 192.168.0.100
WebCam Server - Data Port 5550 192.168.0.100
WebCam Server - Audio Port 6550 192.168.0.100
WebCam Server - SSL Port 443 192.168.0.100
WebCam Server - Mobile Port 8866 192.168.0.100
WebCam Server - Mobile RPB Port 5511 192.168.0.100
14:36:31- Find UPnP Device(1) _(Linksys BEFSR41v3) IP:[221.169.248.174]
14:36:22- Searching for UPnP enabled routers....

Figure 8-17

3. Click **Searching** to search the UPnP-enabled routers.
4. If your server is installed with multiple routers, select a desired one from the UPnP Router drop-down list.
5. If you server is installed with multiple network adapters, select a desired one from the IP Address drop-down list.
6. Click **Configure** to automatically configure the communication ports on the router.

Tip: If you don't use the default ports, modify the related ports in the Server Setup dialog box (Figure 8-5) and then click **OK**. Re-open the dialog box and follow above steps to configure your router.

Note: UPnP technology is also available in other remote applications: Control Center, Center V2, Remote Playback, Authentication Server, VSM and TwinDVR.

8.2.11 FTP Server Settings

You can access the recorded images of JPEG format from a remote computer installed with the FTP server. In Figure 8-10, select the **FTP transfer JPEG file** option, and then click the **FTP Setup** button to display the following dialog box.

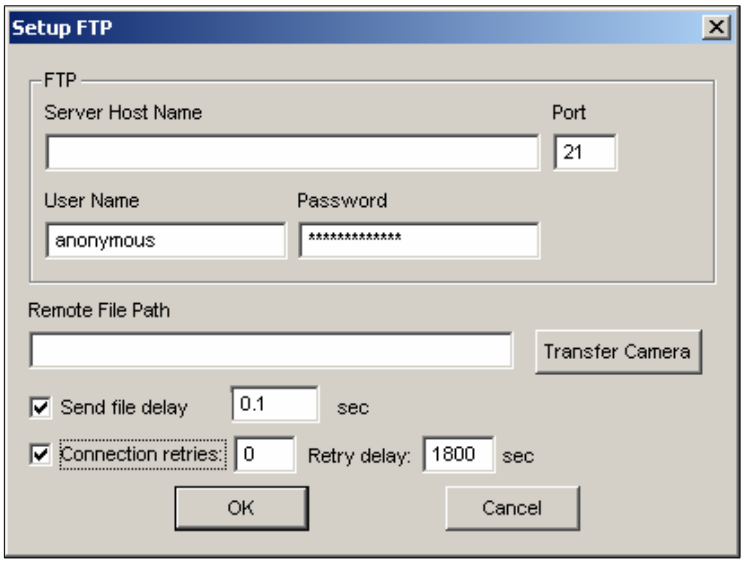


Figure 8-18 *FTP Setup*

1. In the **Server Host Name** field, type the IP address or domain name of the FTP server. Modify the default port value 21 if necessary.
2. Type a login username and password of the FTP server.
3. Specify a file path to save the recorded images on the FTP server.
4. Click the **Transfer Camera** button and assign which camera's files to be transferred to the FTP server.
5. In the **Send File Delay** field, specify the frequency to upload recorded images from the -System to the FTP server. The time range is from 0.1 to 600 seconds.
6. In the **Connection Retries** field, specify the number of retries when the FTP connection fails (Max: 999). In the **Retry Delay** field, specify the interval between each connection retry (Max: 9999 sec.).
7. Click **OK** to apply above settings.

8.2.12 Network Port Information

The Network Port Information is designed for users to view and manage all network ports of remote applications.

On the main screen, click the **Network** button (No. 11, Figure 1-2), and select **Network Port Information**. This dialog box appears.

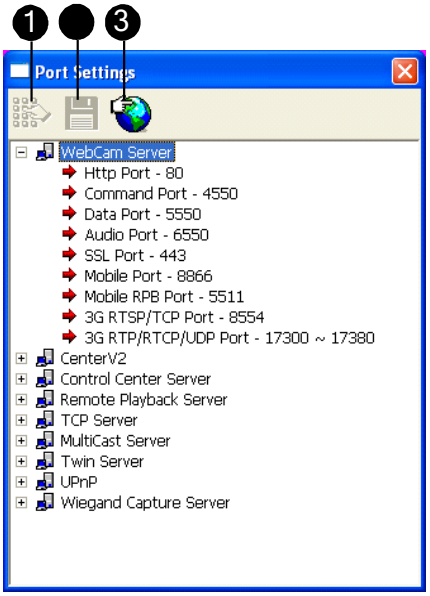


Figure 8-19

The controls on the Port Settings:

No.	Name	Description
1	Modify	Changes the port settings.
2	Save	Saves the port settings.
3	Port Mapping	Employs UPnP technology (Universal Plug and Play) to allow automatic port configuration to the router.

8.3 Single View Viewer

After you log into the WebCam server successfully, you can see the single live view from the -System.

Figure 8-20 *Single View MPEG4 Encoder Viewer*

The controls in the Single View Viewer:

No.	Name	Description
1	Countdown Timer	Indicates the remaining time when you log in as Guest. When time is up, you will be logged out automatically.
2	Menu	Opens the menu of Control Panel. See *Control Panel* later in this chapter.
3	Expand / Close	Expands or closes the Control Panel.
4	Control Panel	See *Control Panel* later in this chapter.
5	Show System Menu	Brings up these options: Alarm Notify, Video and Audio Configuration, Remote Config, Change Server, Show Camera Name and Image Enhance. See *Alarm Notification, Video and Audio Configuration, Remote Configuration, Server List,* and *Image Enhancement* later in this chapter.

6	Change Camera	Selects the desired camera for display.
7	PTZ Control	Displays the PTZ control panel. See *PTZ Control* and *Visual PTZ Control Panel* later in this chapter.
8	I/O Control	Displays the I/O control panel. See *I/O Control* later in this chapter.
9	Full Screen	Switches to full screen view. The maximum video resolution configured on the -System will be applied. See *Video Settings* in *WebCam Server Settings* earlier in this chapter.
10	File Save	Saves live video in the local computer. See *Video Recording* later in this chapter.
11	Change Quality	Adjusts video quality with two options: **Geo H264** and **Geo MPEG4**. For hardware-compressed and megapixel quality, see *Hardware-Compressed and Megapixel Stream* later in this chapter.
12	Snapshot	Takes a snapshot of the displayed live video.
13	Speaker	Enables live audio from the remote -System. See *Video and Audio Configuration* later in this chapter.
14	Microphone	Enables speaking to the remote -System. See *Video and Audio Configuration* later in this chapter.
15	Stop	Terminates the connection to the remote -System.
16	Play	Connects to the remote -System.
17	Live Video	Right-clicking on live video allows you to instantly access some useful functions. The Resolution option can display a resolution indicator at the bottom right corner of the video.

Displaying Full Screen Live View on Another Monitors

Using the IE browser, you can display up to 10 full-screen channels with multiple monitors installed. Right-click the live view and select a designated monitor to bring full screen live view. The full screen live view appears on the designated monitor immediately.

Note: The full-screen display closes at the designed monitor if its Web interface window is minimized.

8.3.1 Control Panel

A control panel is provided for control of the connected channel. To open the control panel, click the **Expand / Close** button (No. 3, Figure 8-19) on top of the Single View viewer. To change the pages of the control panel, click the **Menu** button (No. 2, Figure 8-19). You can also use the right and left arrow buttons on the panel to change the pages.

The functions on the control panel:

Name	Description
Information	Displays the current version, local time, host time and number of channels currently accessing WebCam.
Video	Displays the current video codec, resolution and data rate.
Audio	Displays audio data rates when the microphone and speaker devices are enabled.
Preset Go	Allows you to remotely move the PTZ to the preset points.
I/O Control	Provides a graphic display of the input and output devices from the -System.
Alarm Notify	Displays the captured images by sensor triggers and/or motion detection. See *Alarm Notification* later.
Camera Adjustment	Allows you to remotely adjust image quality by moving the slider to the desired values.
POS/Wiegand	Allows you to view POS transactions or cardholder data along with live video. If the monitoring is activated on the -System, double-clicking any transaction items or cardholder data can have an instant playback.
People Count	Allows you to view the counts of Object Counting along with live view. Once the counts are logged into the -System, **In** and **Out** counts will become zero and the system will start counting those numbers again.

8.3.2 Server List

You can add the connection information of multiple -Systems to the WebCam server for quick access later. Click the **Show System Menu** button (No. 5, Figure 8-20), and select **Change Server** to display the following dialog box.

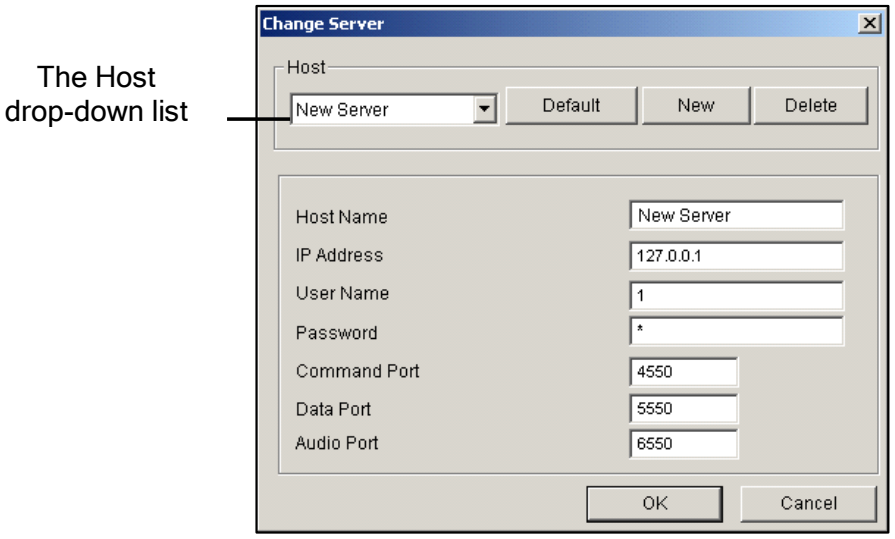


Figure 8-21 *Change Server*

To add a server to the drop-down list, click the **New** button. In Host Name field, type a name to identify the -System. Type the IP address or domain name of the -System. Type a valid username and password to log in to the -System. Leave all port settings as defaults at **4550**, **5550**, and **6550** respectively unless otherwise necessary. Click the **OK** button. Then the created -System will appear in the drop-down list.

8.3.3 Video Recording

Click the **File Save** button (No. 10, Figure 8-20) to save video in a local computer. Files saved in AVI format are playable at third party viewers. Use the slider to adjust the time length of each saved clip.

8.3.4 Alarm Notification

The Single View Viewer can be set to display up to four captured images in the control panel upon motion detection or input trigger. To enable the function, follow these steps.

Figure 8-22

1. Click the **Show System Menu** button (No. 5, Figure 8-20), and select **Alarm Notify.** This dialog box appears.

Figure 8-23 *Alarm Notification*

④ **Motion Notify:** Once motion is detected, the captured images are displayed in the control panel of the Single View.

④ **I/O Alarm Notify:** Once the input device is triggered, the captured images are displayed in the control panel of the Single View.

④ **Alert Sound:** Activates the computer noise alarm on motion and input-triggered detection.

④ **Auto Snapshot:** The program will take a snapshot every 5 seconds on motion and input-triggered detection.

④ **File Path:** Assigns a path to save the snapshots.

2. Click **OK** to apply the above settings.

8.3.5 Video and Audio Configuration

To change the video and audio configurations of the connected camera, click the **Show System Menu** button (No. 5, Figure 8-19), and select **Video and Audio Configuration**.

[Camera]

In this tab, you can change the video codec, quality and frame rate immediately. The resolution options are corresponded to the maximum image size set on the connected -System. For details, see *Video Settings* in *WebCam Server Settings* earlier in this chapter. Note the Defog and Stabilizer options are only available after they are activated at the connected -System.

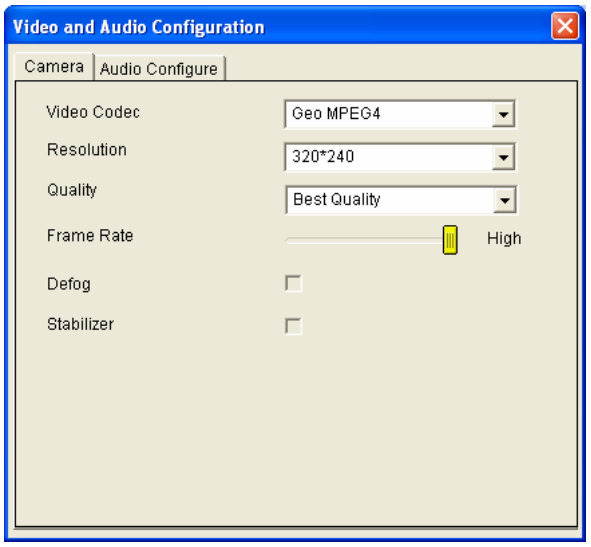


Figure 8-24

[Audio Configure]

In this tab, you can enable the microphone and speaker for two-way audio communication.

Select **Speaker** to access live audio from the server site, and select **Microphone** to speak to the server site. Ensure the speaker and microphone are properly installed in the local computer, and the audio settings (Figure 8-8) are activated on the WebCam server too.

There are three options for audio quality:

- **Real Time:** Transmits simultaneously audio and video but may create sound interruption depending on your network condition.
- **Smooth:** Has a smooth sound quality but without audio and video synchronization.
- **Normal:** The default value which has the audio and video effects between Real-Time and Smooth.

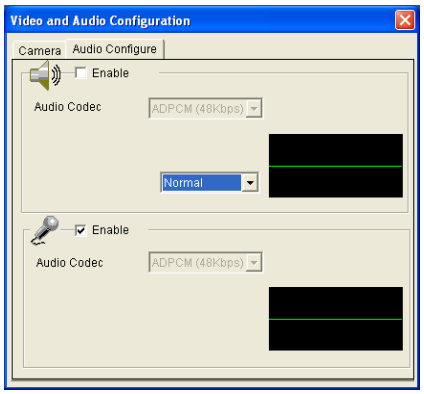


Figure 8-25

8.3.6 Hardware-Compressed or Megapixel Stream

If your video source is of hardware compression or megapixel, you can choose better video quality on the WebCam server. The following conditions can produce a hardware-compressed or megapixel video stream:

1. -4008 Card is installed on the -System.
2. Video sources of the -System are from IP video devices.

To receive hardware-compressed or megapixel stream through the WebCam server:

1. Select **Actual Size** on the -System.
   Click the **Network** button (No. 11, Figure 1-2), select **WebCam Server**, click the **Video** tab and select **Actual Size** in the Max Image Size option. Refer to *Video Settings* in *WebCam Server Settings* earlier in this chapter.
2. On the Single View, click the **Change Quality** button (No. 11, Figure 8-20). You will have the option of megapixel resolution now.

Note:

1. The hardware-compressed and megapixel video stream requires a lot of bandwidth. It is highly recommended to enable this function in a LAN environment.
2. To enable fisheye functions through WebCam server, you must first follow the steps above to set fisheye camera to megapixel resolution. Next, right-click the camera view and select **Geo Fisheye** to see the fisheye settings. For more details on the fisheye settings, see *Fisheye View* in chapter 3.

8.3.7 PTZ Control

Click the **Camera Select** button to select one PTZ camera, and then click the **PTZ Control** button (No. 7, Figure 8-20) to bring up the PTZ control panel.

Figure 8-26 *PTZ control panel*

One PTZ camera only allows one user to control at a time. If several users are trying to control the same PTZ camera at the same time, the Single View viewer will give the priority to the first login user and then to the next user in queue. Each user will be given 60 seconds to control the PTZ camera. The Timer at the upper right corner informs the user of the remaining time of control or the total waiting time.

The supervisor is given the highest priority to control the PTZ camera and won't be restrained by 60-second time limit. When the supervisor logs on the WebCam server, the Timer shows 999.

Click the button to access more functions of the PTZ camera such as changing PTZ speed, starting Auto Scan and setting preset points. The available functions are subject to PTZ models.

To configure preset points for the PTZ camera, ensure the following two settings are enabled first:

1. Map the PTZ camera to a camera channel (Configure button < Accessories < Camera Mapping PTZ Dome).
2. Enable **Remote Control** (Network button < WebCam Server < Enable Remote Control).

8.3.8 Visual PTZ Control Panel

Other than the PTZ control panel, you can display a Visual PTZ Control Panel on the image.

To access this feature, click the **PTZ Control** button (No.7, Figure 8-19) and select **Visual PTZ**. For details on using the Visual PTZ Control Panel, see *PTZ Automation* in Chapter 1.

8.3.9 I/O Control

The new interface provides real-time graphic displays of camera and I/O status, and alarm event. Additionally, you can force output, as well as enable and disable I/O devices to the remote -System. Click the **I/O Control** button (No. 8, Figure 8-20) to bring out the I/O control panel.

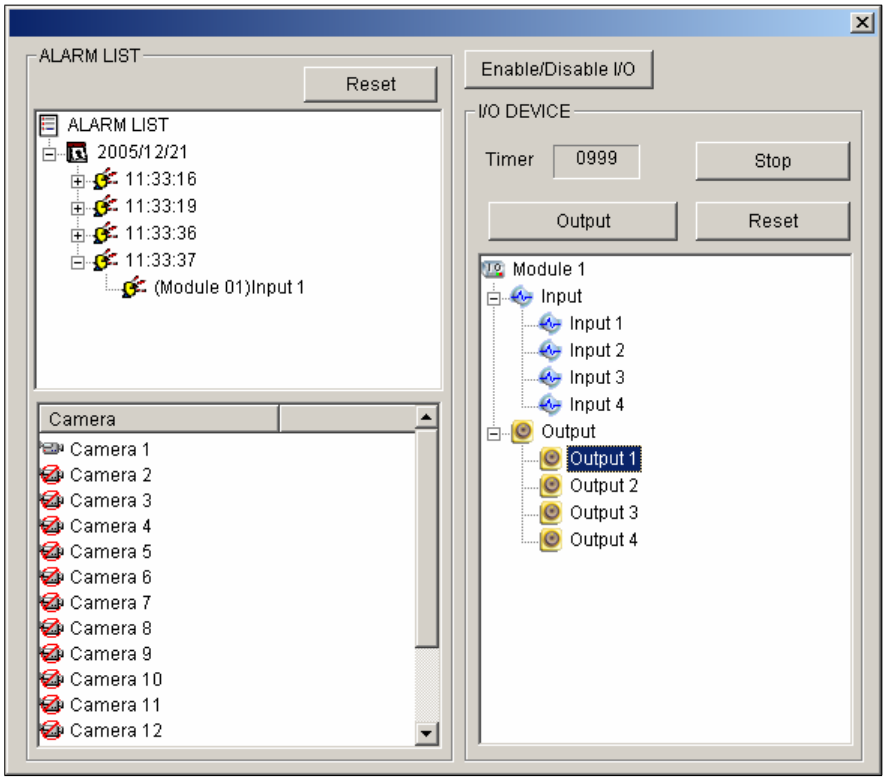


Figure 8-27 *I/O Control*

The alarm status is displayed in three levels. The first level indicates date, second indicates time, and the third indicates alarm ID. Clicking the **Reset** button will clear the alarm list.

To initiate an output device, click the **Enable** button, highlight an output and then click the **Output** button. The Timer functions the same as in the PTZ control panel. Each user will be given 60 seconds of control time while the supervisor has 999 seconds. Clicking the **Stop** button will stop the operation and turn over the control privilege to the next user waiting online.

If you want to enable or disable I/O devices to the remote -System, click the **Enable/Disable I/O** button. For this, the remote -System must grant the privilege first. Enable the **Enable Remote Control** option in Figure 8-5.

8.3.10 Visual Automation

You can remotely change the current status of the electronic device by simply clicking on its image. Moreover, you can manage the settings of Visual Automation.

This feature is only available when the Visual Automation is configured ahead on the -System.

- To access this feature, click the **I/O Control** button (No. 8, Figure 8-20), and select **Visual Automation**.
- Right-click the green **I/O** icon on the left corner to manage the alert areas, such as displaying, embossing and changing colors to alert areas.
- Click the alert areas on the image to force the outputs to be triggered remotely.

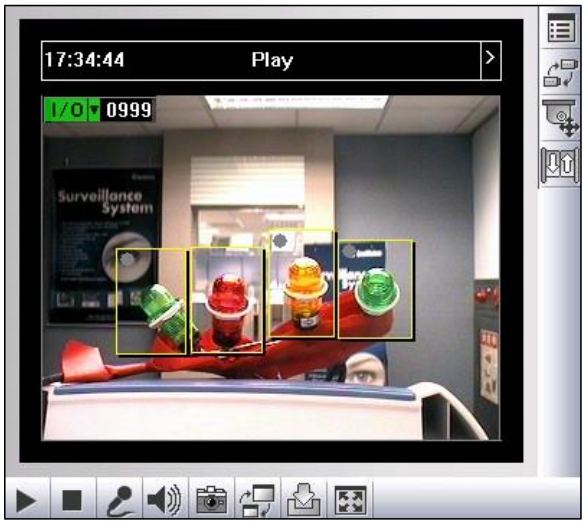


Figure 8-28

8.3.11 Picture-in-Picture View

With the Picture in Picture (PIP) view, you can crop the video to get a close-up view or zoom in on the video. This function is useful for megapixel resolution that provides clear and detailed images of the surveillance area.

To access this feature, right-click on the screen and then select **PIP**. For details on usage, see *Picture-in-Picture View* in Chapter 1.

8.3.12 Picture-and-Picture View

With the Picture and Picture (PAP) view, you can create a split video effect with multiple close-up views on the image. A total of 7 close-up views can be defined. This function is useful for megapixel resolution that provides clear and detailed images of the surveillance area.

To access this feature, right-click on the screen and then select **PAP**. For details on usage, see *Picture-and-Picture View* in Chapter 1.

8.3.13 Image Enhancement

To enhance the image quality of live video, click the **Show System Menu** button (No. 5, Figure 8-20) and select **Image Enhance**. This dialog box appears.

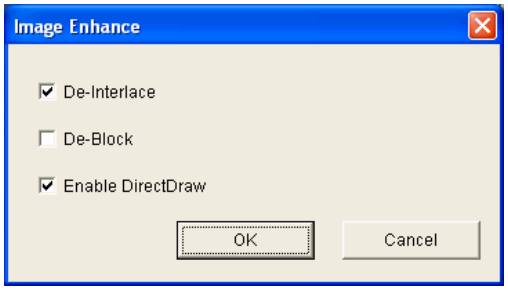


Figure 8-29

④ **De-Interlace:** Converts the interlaced video into non-interlaced video.

④ **De-Block:** Removes the block-like artifacts from low-quality and highly compressed video.

④ **Enable DirectDraw:** The DirectDraw setting is enabled by default. Some VGA cards might not support DirectDraw and can produce distorted frames. Uncheck this option to disable the DirectDraw function.

8.3.14 Remote Configuration

Remote Configuration allows you to start/stop recording, enable/disable I/O monitoring and activate/deactivate schedules to the remote -System. For this, the remote -System must grant the privilege first. See the **Enable Remote Control** option in Figure 8-4.

Click the **Show System Menu** button (No. 5, Figure 8-20) and select **Remote Config** to display the following dialog box.

[Record]

Check the desired cameras to start or stop recording to the remote -System. Click the **Send** button to apply the settings.

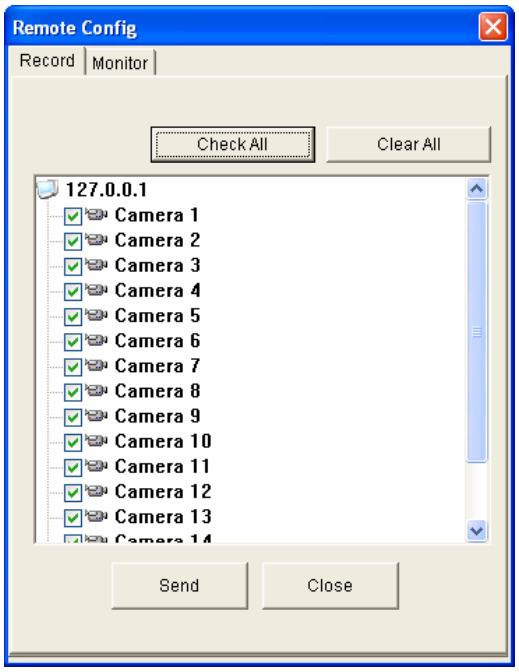


Figure 8-30

[Monitor]

Enable I/O and Schedule monitoring to the remote -System. Click the **Send** button to apply the settings.

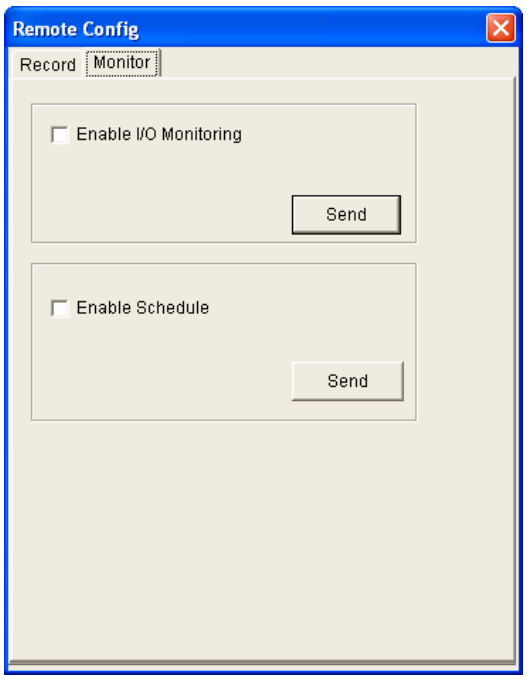


Figure 8-31

8.4 2-Window Viewer

On the 2 Windows, you can drag and drop the **camera**, **PTZ** and **I/O** icons to the desired window for the following functions respectively:

- ⌘ video display
- ⌘ activating the Visual PTZ Control Panel on the image
- ⌘ activating the Visual Automation function

To access the 2 Windows, click **Live View** on the left panel of the Single View page, and then select **2 Windows**.

Figure 8-32

8.5 Multi-Window Viewer

The Multi Windows displays at most 16 channels at a time and supports up to 32 channels.

To access the Multi Windows, click **Live View** on the left panel of the Single View page, and select **Multi Windows**. You can also access Multi Windows directly if you select **Simple Version** at the Login page (Figure 8-2).

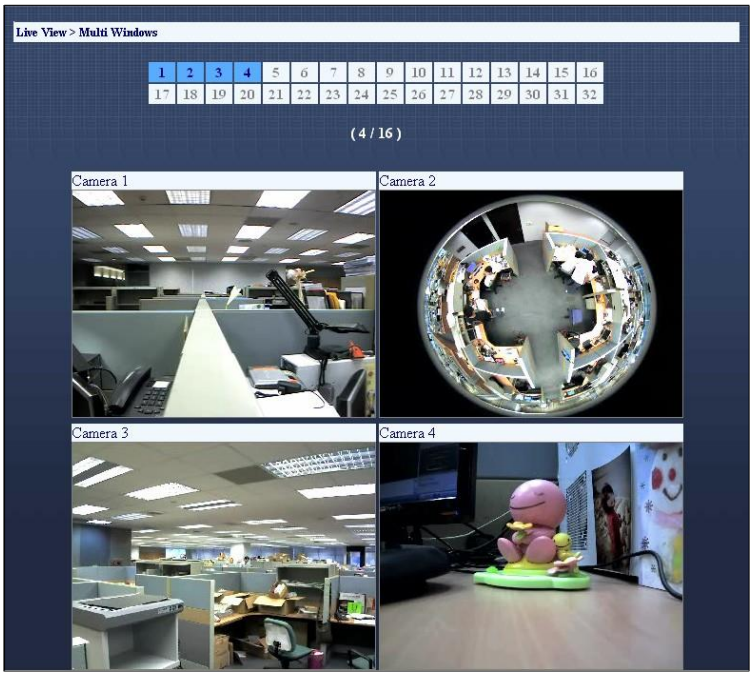


Figure 8-33

8.6 Multi View Viewer

Multi View is a multi-channel viewer, allowing users to view up to 32 live cameras simultaneously. Because multiple channels require a large amount of data to be transferred over Internet, this function is limited to broadband users only.

8.6.1 Installation of Multi View

You can install the Multi View over the Internet or from the Software DVD. The following is an example of installing and running the Multi View over the Internet.

1. On the left panel of the Single View page (Figure 8-20), select **DMMultiView** and select the desired resolution. The first-time user will be prompted to specify a folder to install the Multi View program. When the installation is complete, the Login page appears.

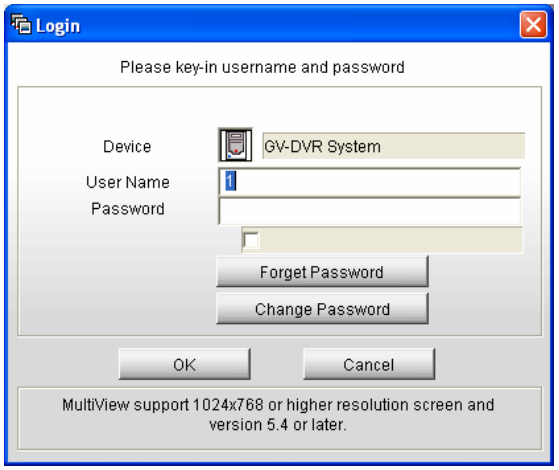


Figure 8-34

2. Type the login **User Name** and **Password** of the -System.
3. Click **OK**. The Multi View window appears.

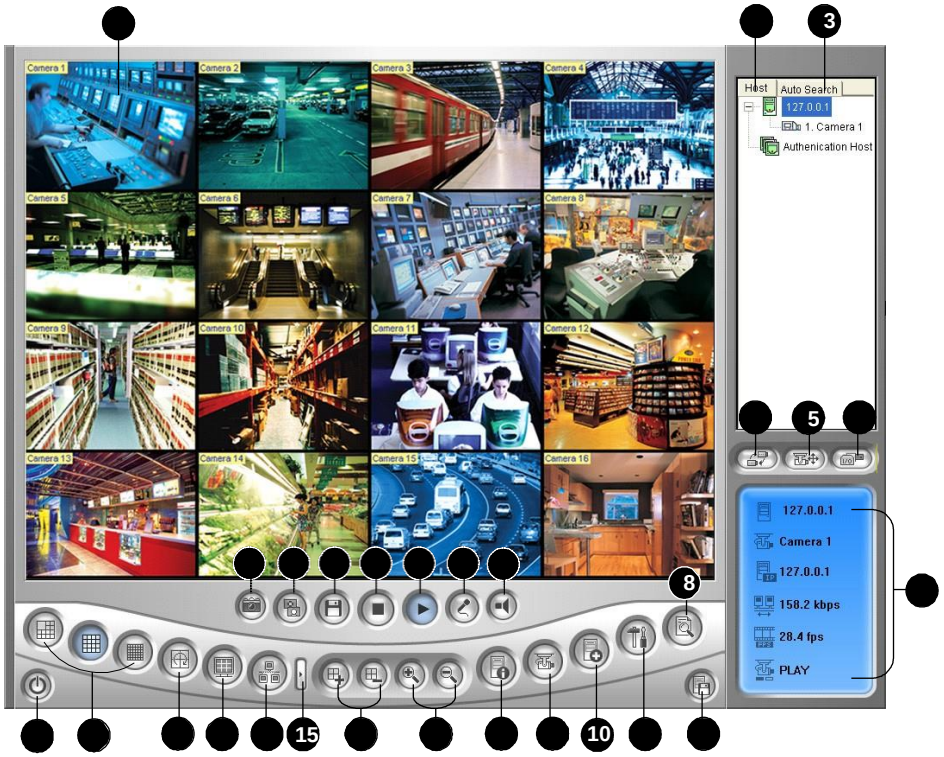


Figure 8-35 *The Multi View Window*

The controls in the Multi View:

No.	Name	Description
1	Monitoring Window	Displays live video. Right-clicking on live video allows you to instantly access some useful functions. Selecting **Resolution** displays a resolution indicator at the bottom right corner of the video.
2	Host List	Displays the connected -Systems and their available cameras. See *Host List* later in this chapter.
3	Auto Search	Displays all hosts on the same LAN. See *Host List* later in this chapter.
4	Show Camera Menu	Select the desired camera for display. If a panorama view is created at the -System, it is also included in this menu.
5	PTZ Control	Displays the PTZ control panel. See *PTZ Control*, and *Visual PTZ Control Panel* later in this chapter.
6	I/O Control	Displays the I/O control panel. See *I/O Control* earlier in this chapter.
7	Channel Status	Indicates the general information of the selected channel. See *Channel Status Information* later in this chapter.

8	ViewLog	Plays back recorded files of the remote -System by using the video player ViewLog. See *Remote ViewLog* later in this chapter.
9	Configure	Accesses system settings of the Multi View. See *System Configuration* later in this chapter.
10	Edit Host	Adds, deletes or modifies a host. See *Creation of a Host* later in this chapter.
11	Camera Status	Displays the camera status of the connected -System. See *Camera Status* later in this chapter.
12	Host Information	Displays the general information of the connected -System. See *Host Information* later in this chapter.
13	Zoom in and out	Zooms in or out the selected channel.
14	Add/Remove Frame	Adds or deletes the frames for video polling. Click the **Add or Remove Frame** button and then click the desired channel to add to or remove from the video polling.
15	Next	Goes to the next page of Screen Division buttons.
16	Multicast	Accesses the Multicast function. See *Multicast and Audio Broadcast* later in this chapter.
17	Full Screen	Switches to a full screen view. The maximum video resolution set on the -System will be applied. See *Video Settings* in *WebCam Server Settings* earlier in this chapter.
18	Video Polling	Rotates through the selected channels. See *Camera Polling* later in this chapter.
19	Screen Division	Sets screen divisions to 4, 6, 8, 9, 10, 13, 16 or 32.
20	Exit/Minimize	Closes or minimizes the Multi View window.
21	Speaker	Enables live audio from a remote -System.
22	Microphone	Enables speaking to a remote -System.
23	Play	Establishes the connection to a -System.
24	Stop	Terminates the connection to a -System.
25	Save	Saves live video. See *Video Recording* later in this chapter.
26	Quality	Adjusts video quality with these options: **Auto Scale** (using the original resolution and quality of video sources), **Geo H264** and **Geo MPEG4**. Display both stream 1 and 2 from IP camera, -Video Gateway and -Recording Server hosts. For hardware-compressed and megapixel quality, see *Hardware-Compressed and Megapixel Stream* later in this chapter.

27	Snapshot	Takes a snapshot of the selected channel.
28	Save Camera to Multiple Host	Saves the selected cameras and creates a Multiple Host. See *Combination of Multiple Hosts into* a *Single Host* later in this chapter.

8.6.2 Host List

The Host List displays a list of available hosts. The host icons indicate available hosts and the camera icons indicate all cameras included in the selected host. To connect to a host:

1. Click a monitoring window, which will be highlighted in red frame.
2. Double-click on a camera icon, and then its corresponding video will be loaded to the selected monitoring window.

First-time users will only see one host icon as no additional hosts are created yet. To create connection to other hosts, see *Creation of a Host* later in this chapter.

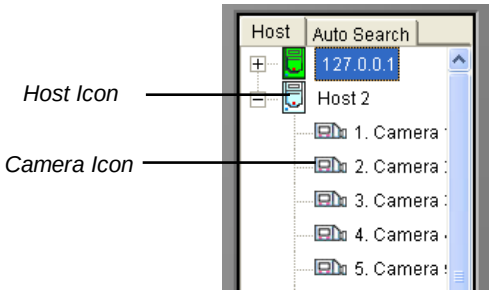


Figure 8-36 *The Host List*

Working with Hosts on the Same LAN

With UPnP technology, Multi View can detect all hosts on the same LAN, without the need of user configuration.

1. On the Host List, click the **Auto Search** tab for detection. A list of hosts within the same LAN appears.
2. Double-click one host for connection. A valid ID and password are required.

Note: For UPnP detection, it is required to open TCP port 5201 on the host and UDP port 5200 on the Multi View site.

8.6.3 Channel Status Information

When choosing a camera from the Host List or the monitoring window, the general information of the selected camera will be displayed in the Channel Status Window as shown below.

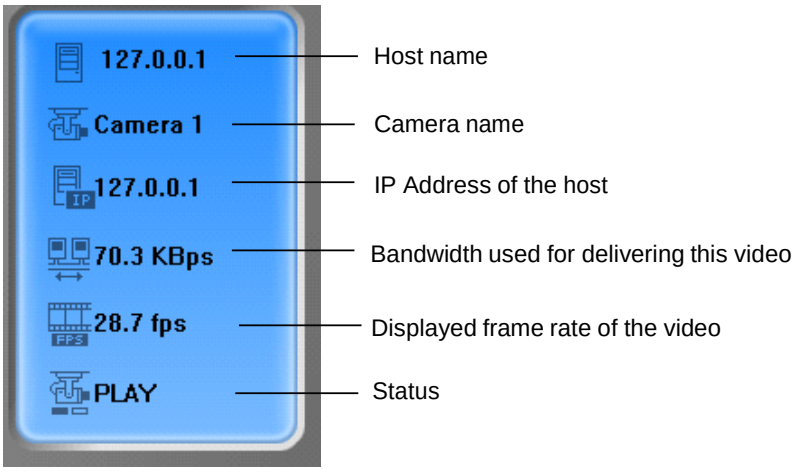


Figure 8-37 *The Channel Status window*

8.6.4 Creation of a Host

The Multi View allows video streaming from multiple -Systems and IP devices. Follow the steps below to create several host accounts for later connection use.

1. Click the **Edit Host** button (No. 10, Figure 8-35). This dialog box appears.

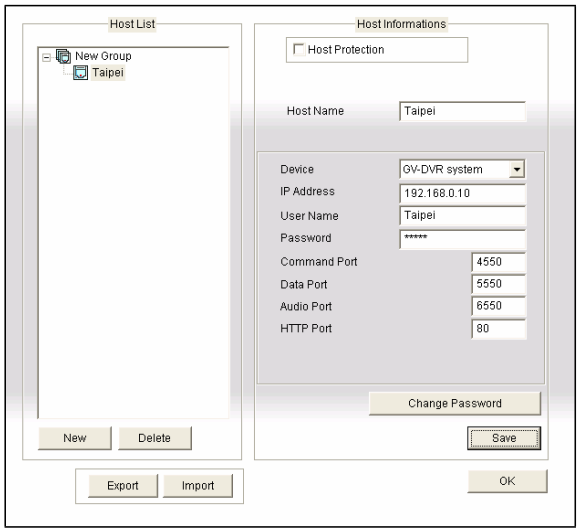


Figure 8-38 *The Edit Host Window*

2. All created hosts are forced to be grouped. Click the **New** button and select **Group** to create a group first. Then click the **New** button again and select **Host** to create a host.
3. In the Host Name field, type a name to identify the host.
4. Select a device type for the host.
5. Type the IP address or domain name of the host. Type a valid username and password to log into the host. Modify the default ports if necessary to match the corresponding ports on the host.
6. Click the **Save** button. The host will appear in the Host List (Figure 8-36) with the given ID name.

8.6.5 Combination of Multiple Hosts into a Single Host

You can combine multiple hosts into a single host including the camera channels all from different IP addresses. There are two methods to combine multiple hosts: the manual creation of Multiple Hosts; the quick creation of Multiple Hosts.

Manual Creation of Multiple Hosts

1. Click the **Edit Host** button (No. 10, Figure 8-35) to display the Edit Host window. Click the **New** button and select **Group** to create a group first. Then click the **New** button again and select **Host** to create a host.
2. Select **Multiple Host**. This dialog box appears.

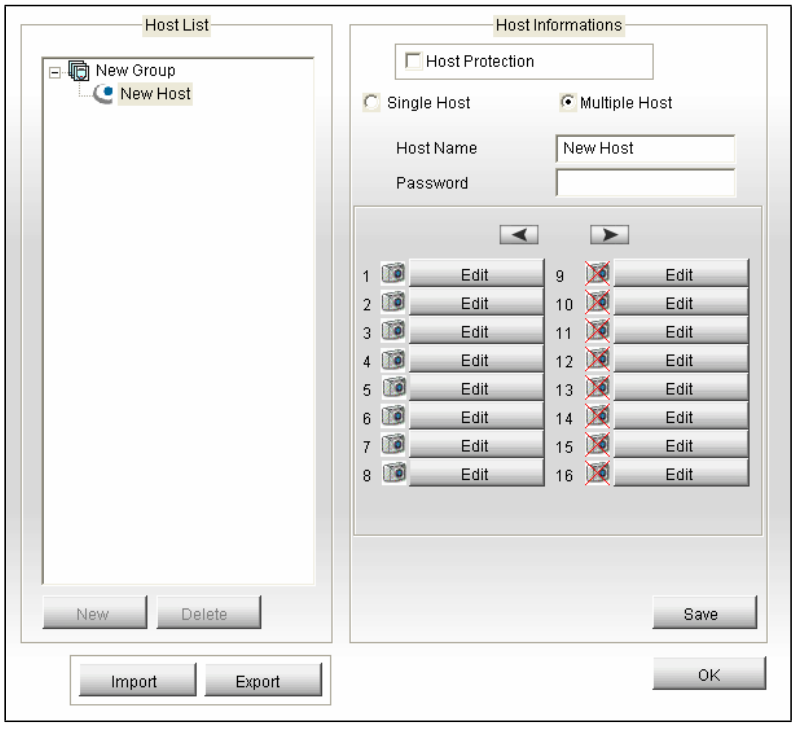


Figure 8-39 *Creating Multiple Hosts*

3. In the Host Name field, enter a desired name to identify the Multiple Hosts.
4. To set up each camera channel of the Multiple Hosts, click the **Edit** tab one at a time. Alternatively, you can click and drag the created camera channel from the Host List (Figure 8-36) to each **Edit** tab. Note that all created camera channels must be added to each **Edit** tab in the order of 1 to 32.

5. Click the **Edit** tab. This dialog box appears.

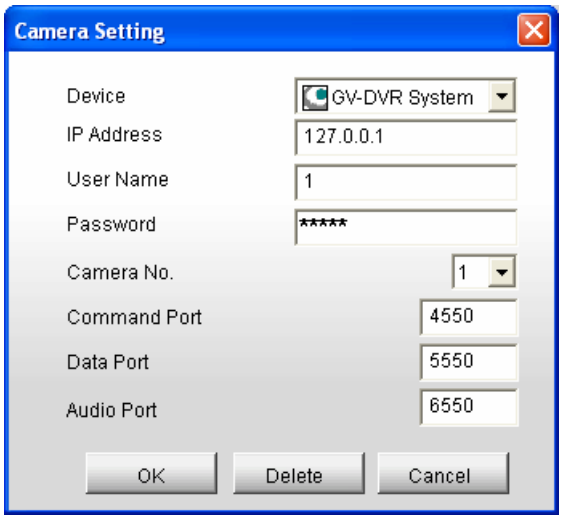


Figure 8-40 *Camera Setting*

6. Select the device type of the host.
7. Enter the IP address, username and password to log into the host.
8. In the **Camera No.** drop-down list, select one desired camera channel from the host.
9. Keep the port settings as defaults; otherwise modify them if necessary.
10. Click **OK**.

Quick Creation of Multiple Hosts

1. Click on a desired monitoring window, which will be highlighted in the red frame.
2. Click and drag a camera from the Host List to the monitoring window. The selected camera then is displayed.
3. Repeat the step 1 and 2 to configure other monitoring windows for different cameras.
4. Click the **Save Camera to Multiple Host** button (No. 28, Figure 8-35) to create the Multiple Hosts.

8.6.6 Video Recording

You can save live videos in a client computer. The files in AVI format are playable at the third party viewer. Click the **Save** button (No.25, Figure 8-35) and then select all or several cameras to start recording. For the recorded folder, see *[Video and Audio]* in *System Configuration* later in this chapter.

8.6.7 Camera Polling

To add cameras to the polling group:

1. Click the **Add Frame** button (No. 14, Figure 8-35), and then click the monitoring windows. The selected windows will be framed in red color.
2. Click the **Video Polling** button (No. 18, Figure 8-35). The application will rotate the selected cameras in the specified time. To configure the polling time, see Figure 8-43.

To remove one camera from the polling group, click the **Remove Frame** button (No. 14, Figure 8-35), and then click its monitoring window.

8.6.8 Hardware-Compressed or Megapixel Stream

To receive the hardware-compressed and megapixel stream from the -System or to enable fisheye functions through WebCam server, refer to the same topic in the section of *Single View Viewer*.

8.6.9 PTZ Control

1. Select a PTZ capable camera from the monitoring window, or double-click it on the Host List (Figure 8-36).
2. Click the **PTZ Control** button (No. 5, Figure 8-35).
3. Turn the switch to the **ON** position.
4. Use the directional, zoom-in, zoom-out, focus-in, focus-out buttons to control the PTZ camera.

The Timer has the same functions as the one in the Single View Viewer. The supervisor is given the highest priority to control PTZ in Multi View and won't be restrained by 60-second time limit. When the supervisor logs in Multi View, the Timer will show 999.

The **Option** button lets you direct the PTZ camera to a preset position and configure the speed of the PTZ camera up to five levels.

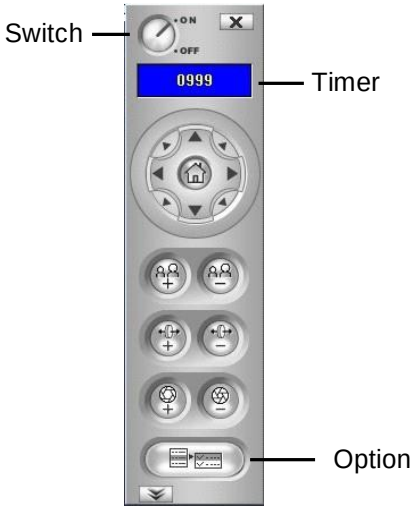


Figure 8-41 *PTZ control panel*

8.6.10 Visual PTZ Control Panel

Other than the PTZ control panel, you can display a Visual PTZ Control Panel on the image.

To access this feature, click the **PTZ Control** button (No.5, Figure 8-20) and select **Visual PTZ**. For details on using the Visual PTZ Control Panel, see *PTZ Automation* in Chapter 1.

8.6.11 Output Control

1. Click the **I/O Control** button (No. 6, Figure 8-35).
2. Turn the switch to ON position.
3. Select a module from the drop-down list. Each module provides 4 to 16 connected relay output devices.
4. Click the **Output (x)** button to enable the output device.

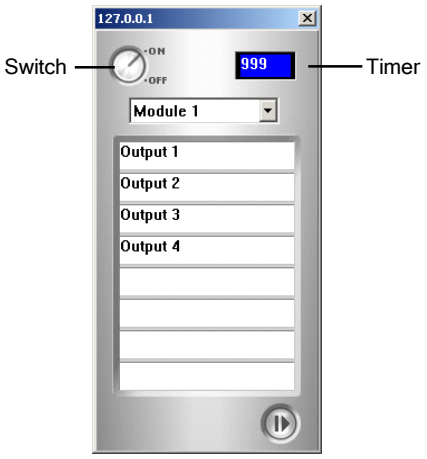


Figure 8-42 *I/O Control Panel*

8.6.12 Remote ViewLog

More than simply playing back recorded video/audio files, the Remote ViewLog function allows you to have full access to the ViewLog features of the connected -System.

Note: To use the Remote ViewLog for the first time, you need to install the Remote ViewLog components to the local PC. Install the components from the Software DVD, or from the Download page (see *Download Center* later in this chapter).

---

1. On the Multi View window, click the **ViewLog** button (No. 8, Figure 8-35). The Connect to Remote ViewLog Service dialog box appears.
2. Type the IP Address, ID and Password of the remote -System. Keep the default port as **5552**, or modify it if necessary.
3. In the Host Type field, select **DVR**.
4. Click the **Connect** button.

When the connection is established, you will see the video player ViewLog appears on the screen. Then you can access all ViewLog features for playback.

8.6.13 System Configuration

Click the **Configure** button (No. 9, Figure 8-35) to display the following window. At the left panel, select **General Display**, **Video and Audio** or **Network** to start your configuration.

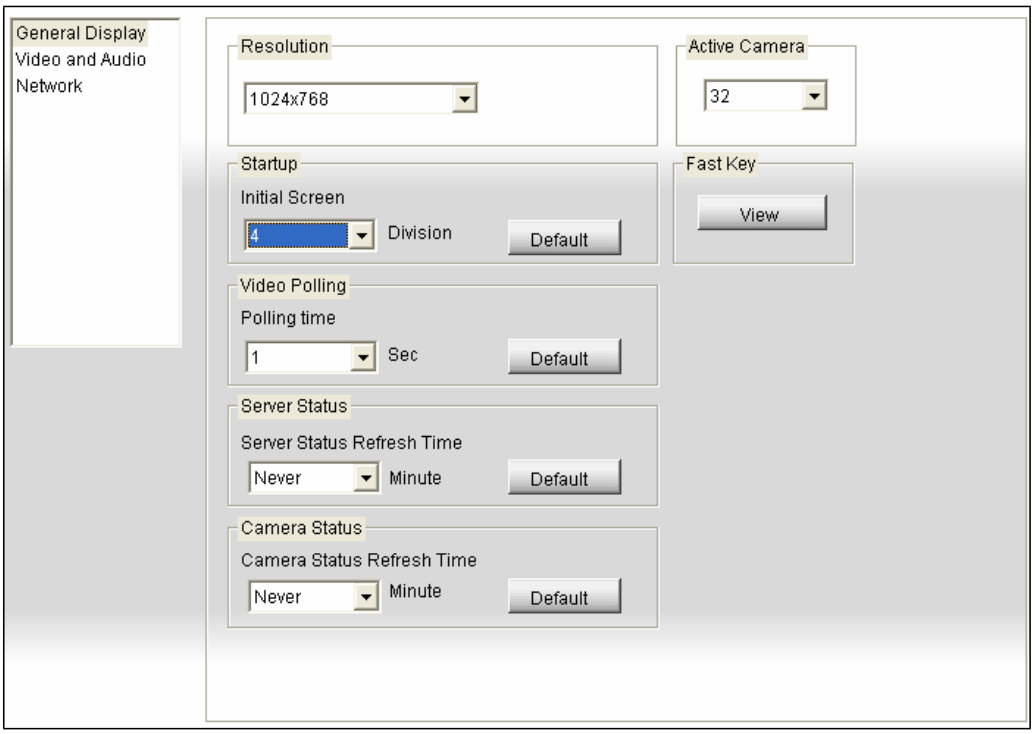


Figure 8-43 *The Configure Window*

[General Display]

④ **Resolution:** Select the Multi View screen resolution. The options available here depend on the monitor resolution of your PC.

④ **Initial Screen:** Select screen divisions at startup.

④ **Polling Time:** Specify the camera polling time from 1 to 60 seconds.

④ **Server Status Refresh Time:** Specify the frequency to update the host information.

④ **Camera Status Refresh Time:** Specify the frequency to update the camera information.

④ **Active Camera:** Select the maximum number of screen divisions allowed on the Multi View.

④ **Fast Key:** Click the **View** button to display the fast key table of the Multi View.

[Video and Audio]

④ **Folder Path:** Specify a path to save recorded files.

④ **Max Video Clip:** Specify the maximum time length of each recorded file.

④ **Audio:** Select the audio quality to be **Normal, Real Time** or **Smooth**. For the details of the three quality options, see *[Audio Configure]* in *Video and Audio Configuration* in the section of *Single View Viewer* earlier in this chapter.

④ **Enable DirectDraw:** See the same features in *Image Enhancement* in the section of *Single View Viewer.*

- **Enable DirectDraw for resolution of 320 x 240 or higher:** Select this option to apply the DirectDraw on the live Images of 320 x 240 or higher resolution. The option conserves the system's CPU resources since the DirectDraw is not applied on the resolution lower than 320 x 240.
- **Enable DirectDraw for all resolutions:** This is the default setting. Select this option to apply the DirectDraw on all live images in any resolution.

④ **Caption:** Select what kind of caption to display on the monitoring window.

[Network] Displays the communication ports of the Multi View.

8.6.14 Camera Status

To show the camera status of the selected -System, click the **Camera Status** button to display the following window. “Camera ON” indicates the camera is active. “No Privilege” means you’re not authorized to view this camera. Clicking the **View** button will bring up a small window displaying the selected camera’s video. Clicking the **Refresh** button will refresh the information in this window.

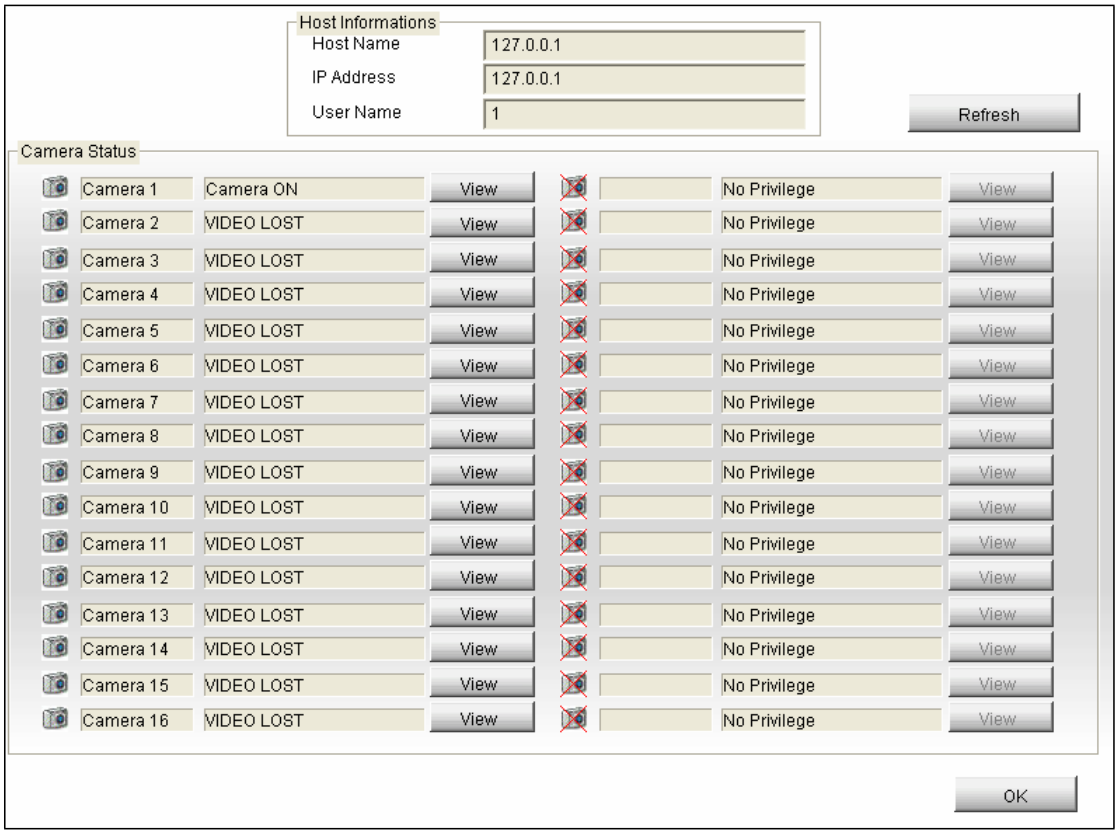

Host Informations
Host Name
127.0.0.1
IP Address
127.0.0.1
User Name
1
Refresh
Camera Status
Camera 1 Camera ON View No Privilege View
Camera 2 VIDEO LOST View No Privilege View
Camera 3 VIDEO LOST View No Privilege View
Camera 4 VIDEO LOST View No Privilege View
Camera 5 VIDEO LOST View No Privilege View
Camera 6 VIDEO LOST View No Privilege View
Camera 7 VIDEO LOST View No Privilege View
Camera 8 VIDEO LOST View No Privilege View
Camera 9 VIDEO LOST View No Privilege View
Camera 10 VIDEO LOST View No Privilege View
Camera 11 VIDEO LOST View No Privilege View
Camera 12 VIDEO LOST View No Privilege View
Camera 13 VIDEO LOST View No Privilege View
Camera 14 VIDEO LOST View No Privilege View
Camera 15 VIDEO LOST View No Privilege View
Camera 16 VIDEO LOST View No Privilege View
OK

Figure 8-44 *The Camera Status Window*

8.6.15 Host Information

To show the host information of the selected -System, click the **Host Information** button (No.12, Figure 8-35) to display the following window. The Host Information window contains the following three categories. Use the control tabs to toggle among them.

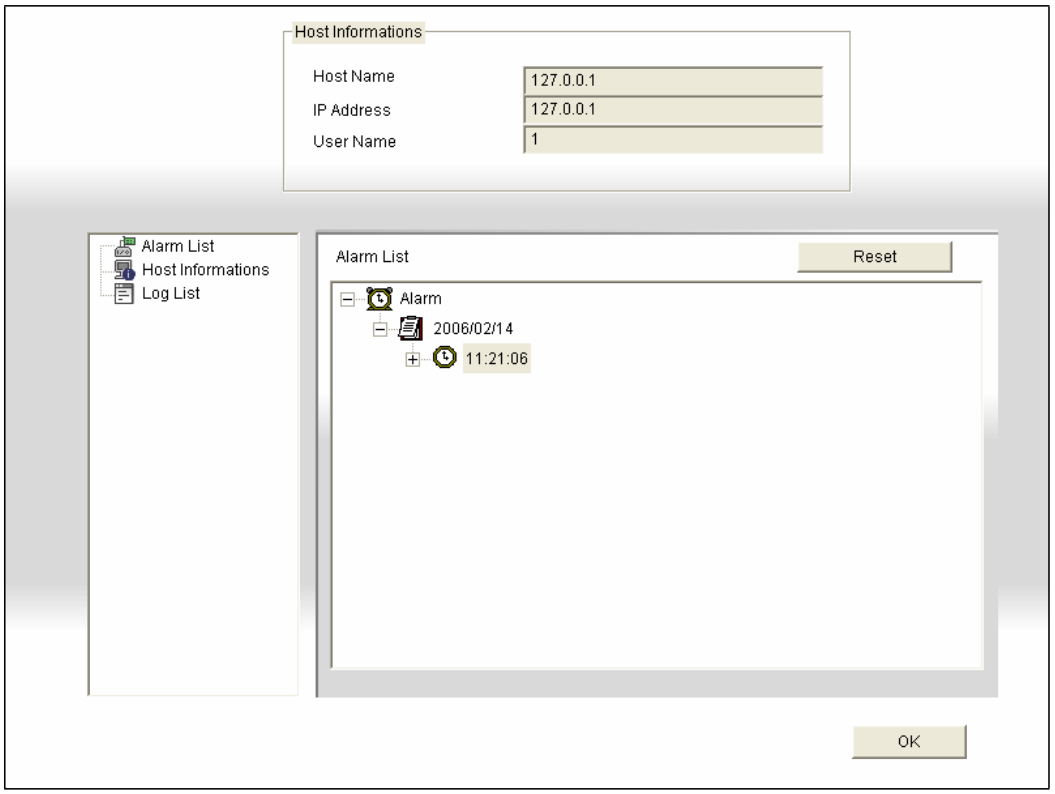


Figure 8-45 *The Host Information Window*

[Alarm List] Displays a list of alarm events occurred in the selected -System. Clicking the **Reset** button will clear the listed events. New events will be generated until the alarms of the remote site are invoked.

[Host Information] The upper section shows the general information of the connected -System. The lower section shows the number of MPEG4, RPB, and audio channels currently serving over the Internet.

[Log List] Displays a history of login and logout information.

8.6.16 Icon Image Change

The icons displayed on the Host List can be replaced with icons of your choice. For example, the figure below has the original Host icon replaced with the icon drawn with a red line across it.

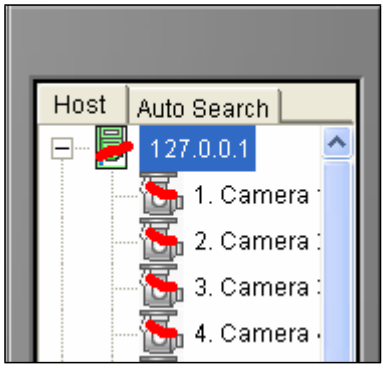


Figure 8-46

Under the DMMultiview folder there are 2 subfolders named, **CommonIcon** and **CustomIcon** (Figure 8-47). Depending on the icons you wish to change, just create a new image icon in **CustomIcon** and rename it to the icon name you wish to replace from **CommonIcon**. To revert back to the original icons, just delete the images in **CustomIcon**. For details on image size restriction and file naming, see *Custom Icon Naming Chart for Multi View* in *Appendix G*.

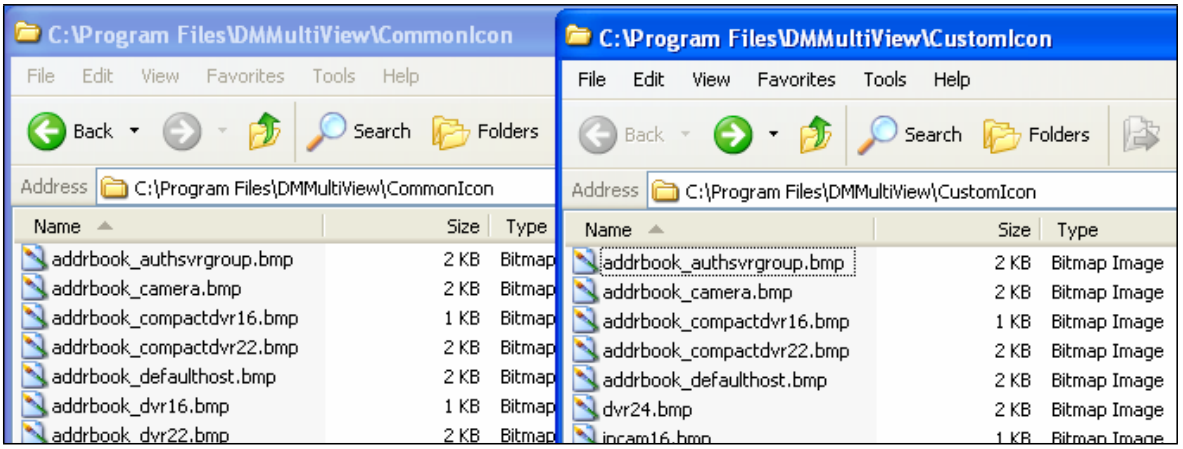

C:\Program Files\DMMultiView\CommonIcon
File Edit View Favorites Tools Help
Back Search Folders
Address C:\Program Files\DMMultiView\CommonIcon
Name Size Type
addrbook_authsvrgroup.bmp 2 KB Bitmap
addrbook_camera.bmp 2 KB Bitmap
addrbook_compactdvr16.bmp 1 KB Bitmap
addrbook_compactdvr22.bmp 2 KB Bitmap
addrbook_defaulthost.bmp 2 KB Bitmap
addrbook_dvr16.bmp 1 KB Bitmap
addrbook_dvr22.bmp 2 KB Bitmap
C:\Program Files\DMMultiView\CustomIcon
File Edit View Favorites Tools Help
Back Search Folders
Address C:\Program Files\DMMultiView\CustomIcon
Name Size Type
addrbook_authsvrgroup.bmp 2 KB Bitmap Image
addrbook_camera.bmp 2 KB Bitmap Image
addrbook_compactdvr16.bmp 1 KB Bitmap Image
addrbook_compactdvr22.bmp 2 KB Bitmap Image
addrbook_defaulthost.bmp 2 KB Bitmap Image
dvr24.bmp 2 KB Bitmap Image
ipcam16.bmp 1 KB Bitmap Image

Figure 8-47

8.7 Multicast and Audio Broadcast

Multicast sends a single video and audio stream to multiple hosts using the same multicast IP address and within the same LAN. Multicast can greatly increase the bandwidth efficiency when multiple hosts access the same video and audio stream.

As for audio broadcast, it allows a host to speak to other hosts using the same broadcast IP address and within the same LAN.

Note: To perform multicast within a LAN with different IP sequence numbers, e.g. 192.168.1.1 and 192.168.2.1, you need a router supporting **Multicast Pass Through** function.

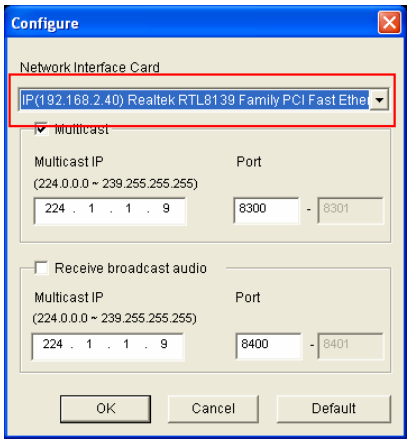
8.7.1 Configuring Multicast and Broadcast Settings

On -System, you can configure two settings. One is to allow remote access to multicast delivered from the -System; the other is to receive audio broadcast from other host.

Activating Multicast

1. Click the **Network** button, select **WebCam Server** and click the **Multicast** tab. The Server Setup dialog box (Figure 8-13) appears.
2. Select **Multicast** to enable the multicast settings.
3. By default the IP address is 224.1.1.2 and port number is 8300 to send the video and audio stream. Modify default values if necessary.
4. Optionally specify a **Password** for hosts to access multicast.
5. Click the **Camera** and **Audio** buttons to select which camera and audio is accessible through multicast.
6. Select another **Network Card**, if available, to run multicast on a different network. Since the multicast can take a lot of bandwidth when enabled, separating it from the main network is advised whenever possible.

Note: If you select different network cards belonging to different networks for multicast, ensure the receiving end of the multicast service is connected to the same network or IP sequence. For example, if the IP address assigned for multicast is 192.168.2.*x*, the receiving end should also use the network card of 192.168.2.*x*.



Network card selection at the receiving end

Receiving Audio Broadcast

1. If you like to receive audio broadcast from other hosts on the -System, select **Receive broadcast audio**. By default the IP address is 224.1.1.3 and port number is 8400 to receive broadcasting. Modify default values if necessary.
2. Click **OK** to start the WebCam server.

Now the -System can not only deliver the multicast stream but receive audio broadcast from other hosts. Ensure a speaker is installed on the -System.

8.7.2 Sending Audio Broadcast

You can start audio broadcasting on any host by installing the following program.

1. Ensure a microphone is properly installed.
2. Install and run **Audio Broadcast** from the Software DVD. This dialog box appears.

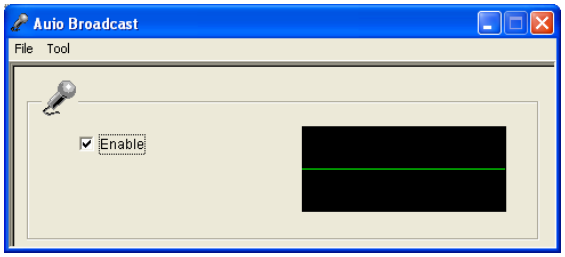


Figure 8-48

3. Select **Enable**. You can start speaking to other hosts.

If you cannot perform audio broadcasting, select **Tool** from the menu bar, select **Set Broadcast Address**, and ensure the IP address and port number are correctly configured. By default the IP address is 224.1.1.3 and port number is 8400 to broadcast audio.

8.7.3 Receiving Multicast and Audio Broadcast

To remotely receive multicast and audio broadcast, there are three methods: use the multicast program included on the Software DVD, through the web interface of WebCam server, and through the Multi View of WebCam server.

Using Multicast Program on Software DVD

1. Install and run **Multicast** from the Software DVD. This dialog box appears.

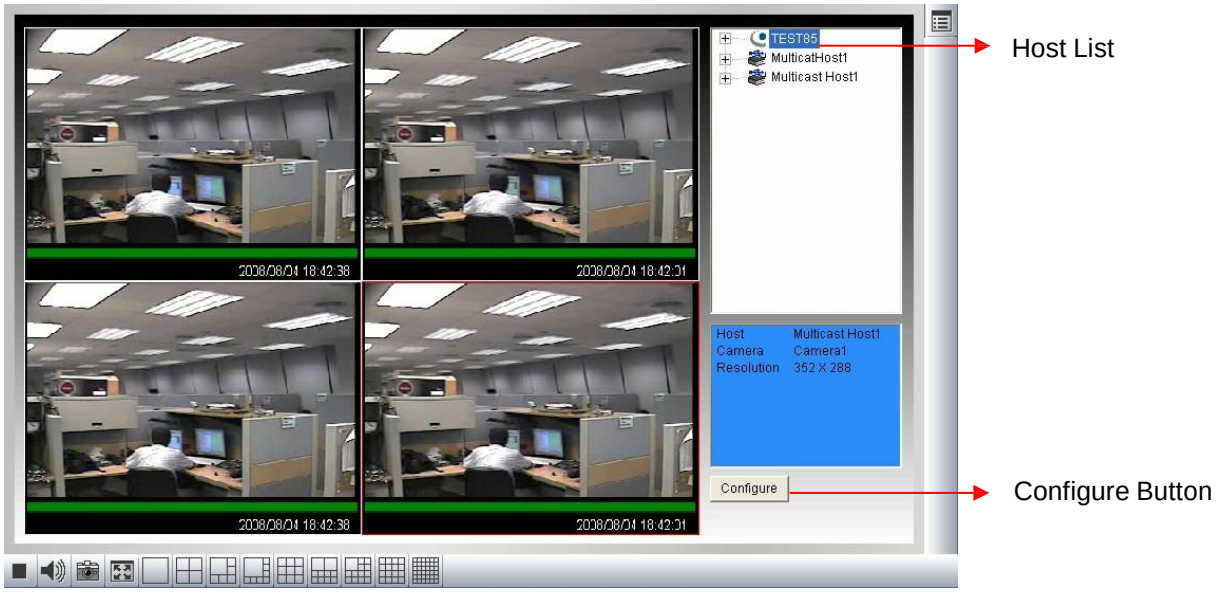


Figure 8-49

2. The host(s), using the same multicast IP address within the same LAN, is displayed automatically on the host list. If you cannot see any host displayed, click the **Configure** button, select **General Setup**, and ensure the relevant IP address and port number are correctly configured.
3. Drag the desired cameras to the screen for display. If the host has already set a password, you will be promoted to enter it at this step.
4. To receive audio broadcast, first ensure a speaker is properly installed on this computer. Click the **Configure** button, select **General Setup**, select **Receive Broadcast Audio**, and ensure the broadcast IP address and port number are correctly configured, and click **OK**.
5. To save the current settings of screen division and camera display for future use, click the **Configure** button, select **Video List Setup**, and select **Export**. You can also select **Import** to apply the pre-defined settings.

Through the Web Interface of WebCam

1. Type the IP address or the domain name of -System on the IE browser. Enter ID and password to log into the -System. When the connection is established, the Single View page appears.
2. On the left panel, select **Live View** and select **Multicast**. The Multicast Viewer (Figure 8-49) appears.
3. To receive multicast and audio broadcast, follow Steps 2-4 in the section of *Using Multicast Program on Software DVD* above.

Through the Multi View of WebCam

1. Click the **Multicast** button (No. 16, Figure 8-35) on the Multi View screen. The Multicast Viewer (Figure 8-49) appears.
2. To receive multicast and audio broadcast, follow Steps 2-4 in the section of *Using Multicast Program on Software DVD* above.

8.8 JPEG Image Viewer

JPEG Image Viewer is a cross-platform viewer, practicable on Mac OS, Netscape, and Microsoft IE browsers. Continuously receiving JPEG images from -System and limited to the single camera view, the viewer is an ideal tool for the users with limited Internet bandwidth.

Note: To enable the JPEG Image Viewer, Java needs to be installed on the local PC.

To start the JPEG Image Viewer, follow these steps:

1. To enable the function on the WebCam server, click the **Network** button, select **WebCam Server**, disable **Enhance Network Security** on the General tab (Figure 8-5), and enable **Create JPEG/GIF File(s)** on the JPG tab (Figure 8-10).
2. Open an Internet Explorer browser on the local PC.
3. Enter the IP address or domain name of the -System. The Single View page (Figure 8-20) appears.
4. On the left panel, click **Live View** and select **JPEG Image Viewer**. A valid ID and a password are required for login. The JPEG Image Viewer window appears.

Figure 8-50 *JPGE Image Viewer*

8.9 Remote Playback

With the Remote Playback (RPB) function on the WebCam server, you can play back the recorded files of the connected -System.

To allow remote access to -System, ensure the WebCam server with the **Run ViewLog Server** function (Figure 8-4) is activated on -System.

1. In the left panel of the Single View page (Figure 8-20), click **Remote Play Back** and select **Remote Play Back**. This window appears.

Figure 8-51

2. Select the desired camera, date and time-segment file.
3. Click the **Play** button to start.
4. For further playback features, click on the image to have the options of **Play Mode, Render** and **Tools.**

8.10 Remote ViewLog

Through WebCam Server, you can remotely play back the recorded files by using the video player ViewLog.

To allow remote access to -System, ensure the WebCam server with the **Run ViewLog Server** function (Figure 8-5) is activated on -System.

1. On the left panel of the Single View page (Figure 8-20), click **Remote Play Back** and select **ViewLog**. This dialog box appears.

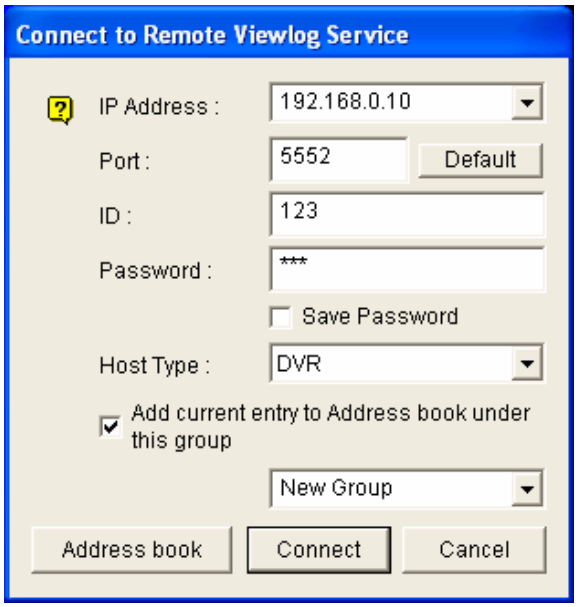


Figure 8-52

2. Type the IP Address, ID and Password of the -System. Select **DVR** to be the host type. Keep the default port as **5552**, or modify it if necessary.
3. Click the **Connect** button.

When the connection is established, you will see the video player ViewLog appears on the screen. Then you can access all ViewLog features for playback.

8.11 Event List Query

With the Event List Query function on the WebCam server, you can remotely locate a desired event by defining search criteria. The search results can be displayed in a text form or a statistic chart. You can also play back any suspicious events instantly.

To allow remote access to -System, ensure the WebCam server with the **Run ViewLog Server** function (Figure 8-5) is activated on -System.

1. On the left panel of the Single View page (Figure 8-20), click **Remote Play Back** and select **Event List Query**. The Query window appears.
2. On the left panel, select one of the following query categories, and then click **Submit Query** at the button of the panel to change the category:
   - ④ **Monitor:** monitored events
   - ④ **System:** system activities
   - ④ **Login:** user login/logout status
   - ④ **Counter:** counter events
   - ④ **POS:** POS transaction events

   Note that the above categories are based on those of System Log in the Main System, so you can also locate the same event recorded in System Log.
3. Define the search criteria such as Event Type, Device, Information, Date and etc. The selection of search criteria may vary depended on query categories.
4. If you search the events recorded during the Daylight Saving Time period, select **DST Rollback** and define a certain period of time in the Date column.
5. Click **Submit Query**. The search results will be displayed in the text form.
6. To play back the attached video, click the **Video** icon.

   Righting-click on the video image gives you more playback features, such as changing playback mode and turning on audio if available.
7. To graph the search results, click the **Chart** button.

8. To export the search results, select one of formats Txt, Html or Excel and then click the **Export** button.

Figure 8-53

8.12 Download Center

The Download Center provides you with an easy option to upgrade the codec, and decide what kind of viewing program should be downloaded to your local computer based on screen resolution required.

1. Click **Download** in the left panel of the Single View page (Figure 8-20). This page appears.

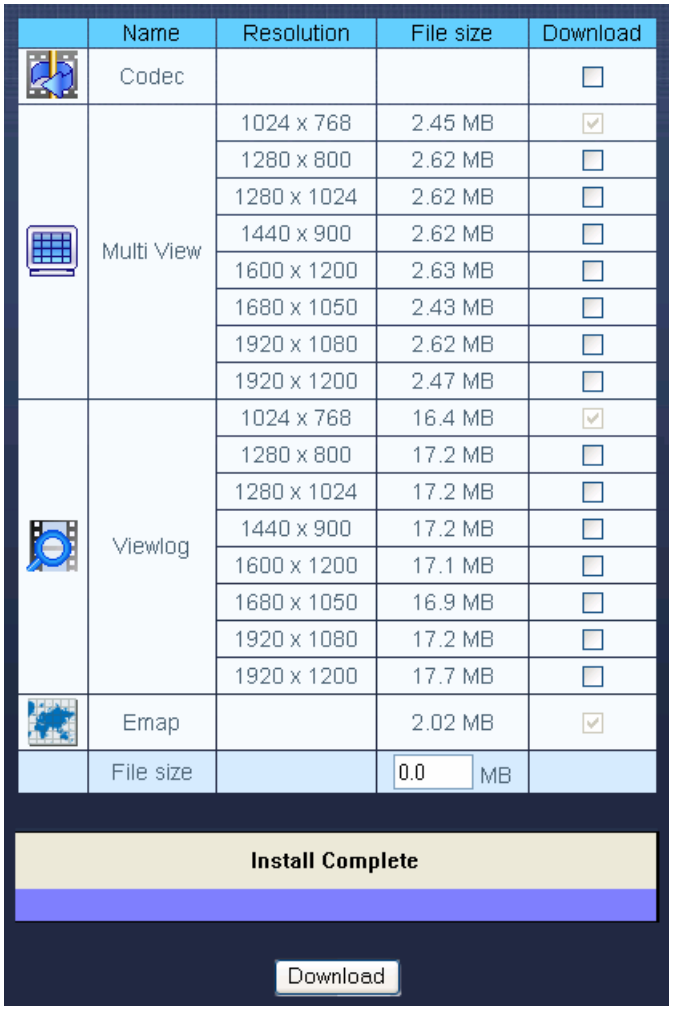


Figure 8-54

2. Check the desired programs. The **File Size** field will display the total file size of the selected programs.
3. Click **Download** and follow the on-screen instructions to install the programs. When the installation is complete, the message "*Install Complete*" will be displayed.

8.13 Mobile Phone Applications

With the mobile phone capable of GPRS, 3G and Wi-Fi, you can receive live videos from your -System. The mobile phone applications and their major features are listed below.

Overview of Mobile Phone Applications

Handheld Device View	**-iView V2.3 for iPhone and iPod Touch**
OS Supported	**iPhone** with iOS 4.3.3 to 6.1.3 **iPod Touch** with iOS 4.3.3 to 6.1.3
Port	Data Port: 8866, RPB Port: 5511, HTTP Port: 80; Command Port: 4550 (for PTZ control); Data Port: 5550 (for PTZ control)
Protocol	TCP/IP (MJPEG)
Resolution	QCIF (160 x 120), CIF (320 x 240), VGA (640 x 480)
Functions	Video Streaming, Remote Playback (RPB), PTZ control, I/O Trigger, Multiple Camera Views and Snapshots.
Handheld Device View	**-iView HD V1.2 for iPad**
OS Supported	iPad with iOS 4.3.3 to 6.1.3
Port	Data Port: 8866, RPB Port: 5511, HTTP Port: 80; Command Port: 4550 (for PTZ control); Data Port: 5550 (for PTZ control)
Protocol	TCP/IP (MJPEG)
Resolution	QCIF (160 x 120), CIF (320 x 240), VGA (640 x 480)
Functions	Video Streaming, Remote Playback (RPB), PTZ control, I/O Trigger, Multiple Camera Views and Snapshots.
Handheld Device View	**-AView V1.3.1 for Android Smartphone**
OS Supported	Android version 2.2 to 4.1.2
Port	Data Port: 8866, RPB Port: 5511, HTTP Port: 80
Protocol	TCP/IP (JPEG)
Resolution	QCIF (176 x 144), CIF (320 x 240), VGA (640 x 480)
Functions	Video Streaming, Remote Playback (RPB), PTZ control, I/O Trigger, Multiple Camera Views and Snapshots.

Note:

1. The remote playback (RPB) function does not support the playback of video files recorded on the IP devices.
2. For -AView, PTZ control is only supported in -PT110D, -PTZ010D, -IP Speed Dome and COP 15-CD53W (Pelco D).

8.13.1 iPhone, iPod Touch, and iPad

-iView function is introduced to support iPhone, iPod Touch, and iPad for the mobile surveillance application. For the supported operating system version, see the *Overview of Mobile Phone Applications* chart earlier in this chapter.

Installing -iView

You can download -iView from **App Store** and install the application. The -iView icon will appear on the desktop.

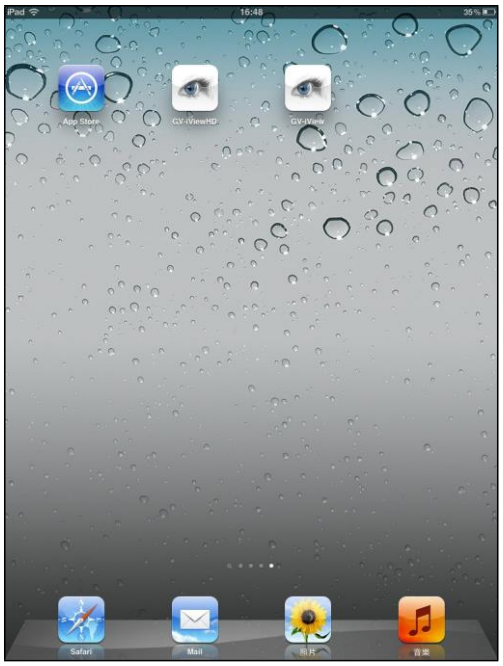


Figure 8-55

Activating the -iView Function

To access the -System from -iView, you need to first activate the JPG settings and the mobile function on the -System.

1. On the main screen, click the **Network** button, select **WebCam Server**.

2. In the dialog box that appears, click the **JPG** tab, and select **Create JPEG/GIF file(s)**.

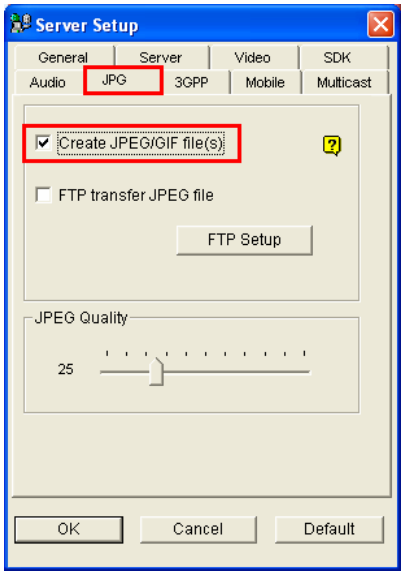


Figure 8-56

3. Click the **Mobile** tab and select the checkbox to enable the mobile function.

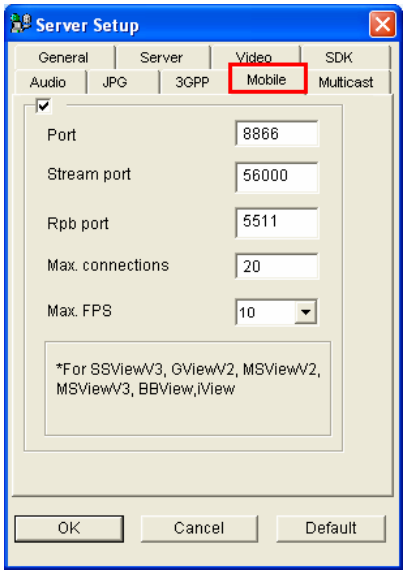


Figure 8-57

4. Click **OK** to save the settings.

Note: If there is a router or firewall installed, ensure these communication ports required by the WebCam server are open: HTTP Port 80, HTTPS Port 443 (if SSL is enabled), Live View Port 8866 and RPB Port 5511.

Connecting to -System

1. On your mobile phone, tap the **-iView** icon on the main screen. This page appears.

Figure 8-58

2. On the login screen, enter the IP address of the -System, port value (default value is 8866), ID and Password. Then tab Connect. Once the connection is established, the live display of 6 cameras will appear.

3. Select ON for HTTPS if SSL is enabled for WebCam Server. If the default SSL port of 443 on the WebCam Server is modified, specify the new port number used for HTTPS connection at the end of the IP address, e.g., webcam.Sting Alarm.com.tw:445.

Note: If the default HTTP port of 80 on the WebCam Server is modified specify the new port number used for HTTP connection at the end of the IP address, e.g., webcam.Sting Alarm.com.tw:81.

For details on accessing live view, playing back recording and other functions, visit the link below and click **Installation Guide** under -iView::

http://www.Sting Alarm.com.tw/english/5_4_iview.asp

8.13.2 Android Smartphones and Tablets

-AView function is introduced to support Android smartphones and tablets for the mobile surveillance application. For the supported operating system version, see the *Overview of Mobile Phone Applications* chart earlier in this chapter.

Installing -AView

You can download -AView from Android Market and install the application. The -AView icon will appear on the desktop.

Figure 8-59

Activating the -AView Function

To access the -System from -AView, you need to first activate the JPG settings and the mobile function on the -System.

1. In the main system, click the **Network** button and select **Webcam Server**.

2. In the dialog box that appears, click the **JPG** tab and select **Create JPEG/GIF file(s)**.

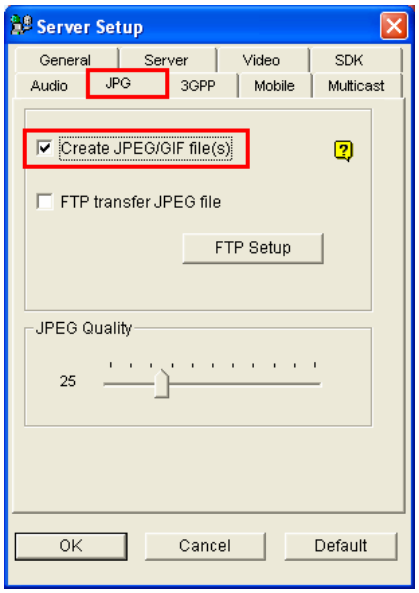


Figure 8-60

3. Click the **Mobile** tab and select the checkbox to enable the mobile function.

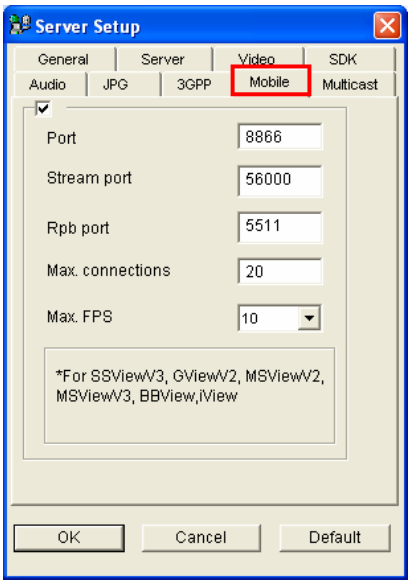


Figure 8-61

4. Click **OK** to save the settings.

Note: If there is a router or firewall installed, ensure these communication ports required by the WebCam server are open: HTTP Port 80, HTTPS Port 443 (if SSL is enabled), Live View Port 8866 and RPB Port 5511.

Connecting to -System

1. On your mobile phone, tap the -AView icon on the main screen and tap the NVR/DVR View tab. This page appears.

Figure 8-62

2. Type the IP address, port number, user name and password of the -System you want to access. And then tap the **Add** button to save the connection information in the address book.

3. Select **ON** for HTTPS, if SSL is enabled for the WebCam Server. If the default SSL, port of 443, on the WebCam Server is modified, type the new port number at the end of the IP address and use a colon to separate the port number from the IP address for HTTPS connections, e.g., webcam.Sting Alarm.com.tw:445.

Note: If the default HTTP port of 80 on the WebCam Server of the -System is modified, specify the new port number used for HTTP connection at the end of the IP address, e.g., webcam.Sting Alarm.com.tw:81.

---

4. Tap the created link in the address book.

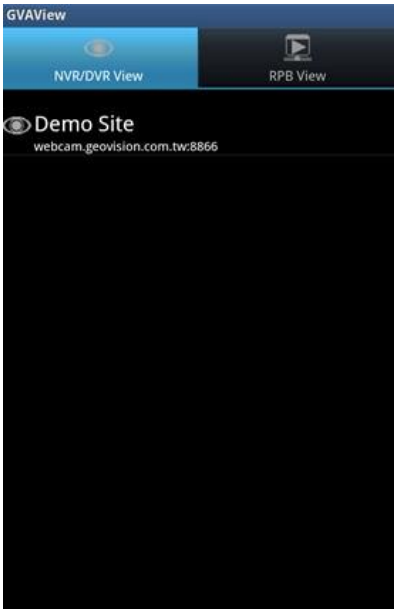


Figure 8-63

5. Tap the **Connection** button to access the -System.

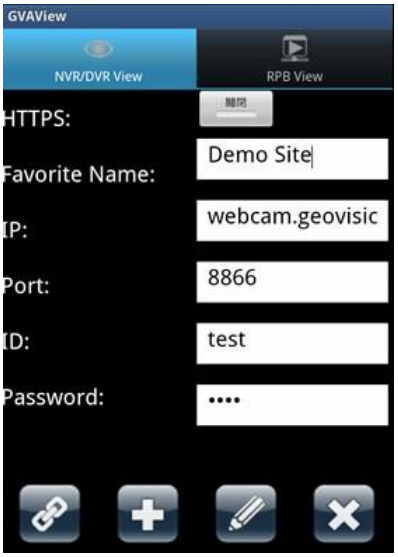


Figure 8-64

For details on accessing live view, playing back recording and other functions, visit the link below and click **Installation Guide** under -AView:

http://www.Sting Alarm.com.tw/english/5_4.asp

8.14 Web Browsers on Smartphones

Using the browser on your smartphone, you can watch live view, control PTZ live views, and play back recordings from a -System. By connecting to the WebCam server, no extra application is required.

Note:

1. Make sure the 3GPP function is enabled at the WebCam server.
2. Live view control is only available for supported PTZ cameras. For the support list, see *Appendix B*.
3. The playback function is only supported by Android devices.

In the following steps, we use the Android smartphone as an example to log in the -System:

1. Open the browser on your Android device and type the IP address of the -System to log in.

Figure 8-65

2. Click **Login**. The cameras on the -System appear.

Figure 8-66

3. To watch live view, tap **Live View** on the top, tap the **H.264** option for **Streaming Type** and then tap a **video** icon . The device connects to the live view shortly.
4. To access the PTZ functions, tap **Live View** on the top and then tap the **JPEG** option for **Streaming Type**. This page appears. You can control the live view with the direction arrows, zoom in/out and home position buttons.

Figure 8-67

5. To play back, tap **Remote Play Back**. This page appears. Search recordings by defining the camera, date and start time. If the video is recorded on a Daylight Saving day, select **Yes** for **DST Rollback.**

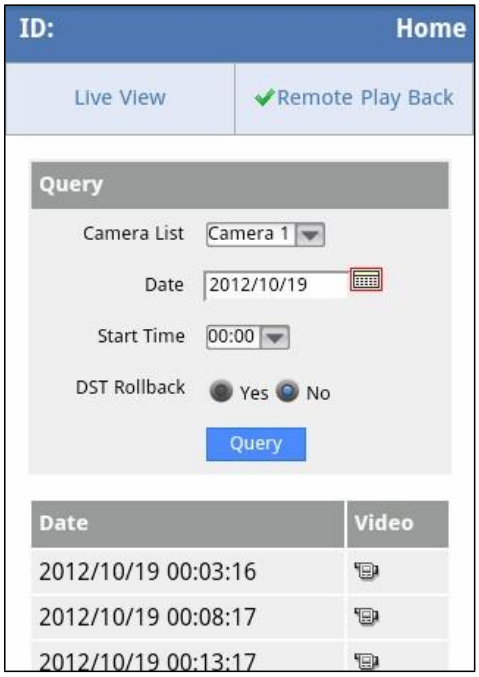


Figure 8-68

The matched results are shown. Click the **video** icon for instant playback.

Chapter 9

E-Map Application.....463

9.1 The E-Map Editor 463

9.1.1 The E-Map Editor Window 464

9.2 Creating an E-Map File 465

9.2.1 Creating an E-Map File for a Remote Host 467

9.2.2 Setting Polygonal Map to Locate a Triggered Device 468

9.2.3 Setting View Zone to Show the Monitored Area 469

9.3 Starting E-Map 470

9.3.1 Setting the Pop-up Map Function 471

9.4 Starting E-Map from a Remote Site 472

9.4.1 The Remote E-Map Window 472

9.4.2 Logging in Different Hosts 474

9.4.3 Configuring the Remote E-Map 475

9.4.4 Viewing Host Information and Playing Back Video 476

9.4.5 Accessing Remote ViewLog 477

9.5 E-Map Server 478

9.5.1 Installing E-Map Server 478

9.5.2 The E-Map Server Window 479

9.5.3 Setting E-Map Server 480

9.5.4 Remote Monitoring via E-Map Server 481

9.5.5 Accessing Authentication Server Account Information 482

CHAPTER

9

E-Map Application

E-Map displays the monitoring area on an electronic map, by which the operator can easily locate the cameras, sensors and alarms triggered by motion or I/O devices. Topics discussed in this chapter include: creating an E-Map file with E-Map Editor, working with E-Map in the Main System, working with E-Map on the WebCam server and E-Map Server.

9.1 The E-Map Editor

The E-Map Editor program allows you to import a floor plan in BMP, GIF and JPG formats, and use the icons of cameras and I/O devices to edit a map per your requirement.

The E-Map Editor program comes with the installation of Main System. Click the Windows **Start** menu, select **Programs**, select **folder** and click **EMap Editor**. The E-Map Editor window will appear.

9.1.1 The E-Map Editor Window

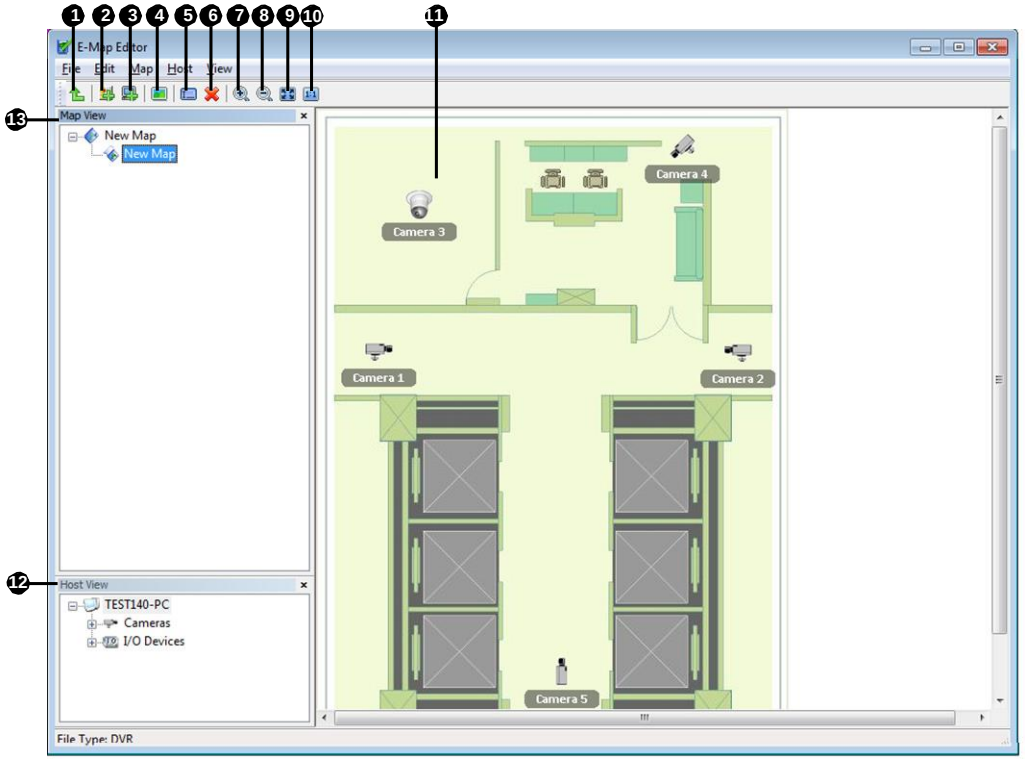


Figure 9-1 *The E-Map Editor Window*

The controls in the E-Map Editor window:

No.	Name	Description
1	Up	Returns to the previous E-Map file.
2	Add Map	Adds an E-Map file.
3	Add Host	Adds a host folder in the Host View.
4	Load Map	Imports a floor plan.
5	Rename	Renames an E-Map file and/or folder.
6	Delete	Deletes an E-Map file and/or folder.
7	Zoom In	Enlarges the Map View.
8	Zoom Out	Diminishes the Map View.
9	Fit to Screen	Adjusts the Map View to fit the current size of the window.
10	Actual Size	Displays actual size of the imported graphic file.
11	Floor Plan	The window displays the imported graphic file.
12	Host View	Tree view of host folders.
13	Map View	Tree view of E-Map files and/or folders.

9.2 Creating an E-Map File

To create and edit an E-Map file, follow the steps below.

1. Click the **Add Map** button (No.2, Figure 9-1) on the toolbar. A New Map file will be created in Map View and the Floor Plan window separately, as illustrated below.

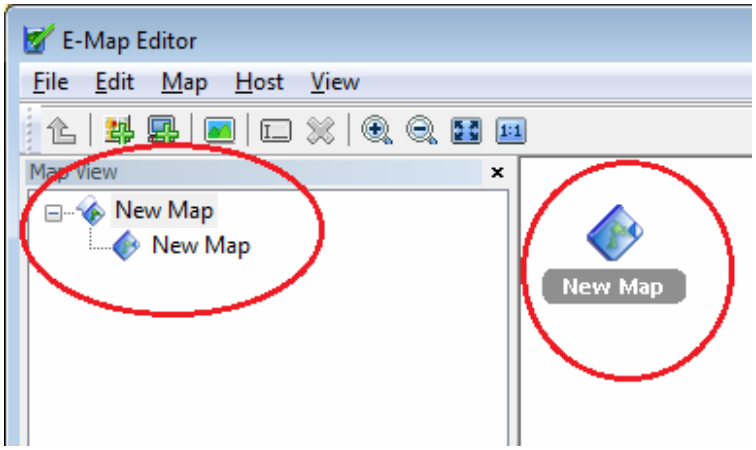


Figure 9-2 *Creating a new map*

2. Click the **New Map** file in Map View, and then click the **Load Map** button (No. 4, Figure 9-1) to import a graphic file. The file opens in the Floor Plan window (Figure 9-1).
3. Double-click the local server folder in Host View. The program will automatically detect the number of cameras and I/O devices already installed at the server, and display their separate icons.
4. Drag and drop these icons from Host View onto the map in the Floor Plan window.
5. The E-Map Editor lets you set the orientation of camera icons and change the icons. Right-click any camera icon to call up a menu, and select the direction where you want the camera to point to. Or change the camera icon into the dome icon.

6. To change the icons for I/O devices, right-click any I/O device icon on the map and select **Change Icon**. The window below appears. Click **No Event** and select an icon to display when the I/O device is not triggered. Click **Event** to select an icon to display when the I/O device is triggered. You can use your own icon by clicking **Add Icon**.

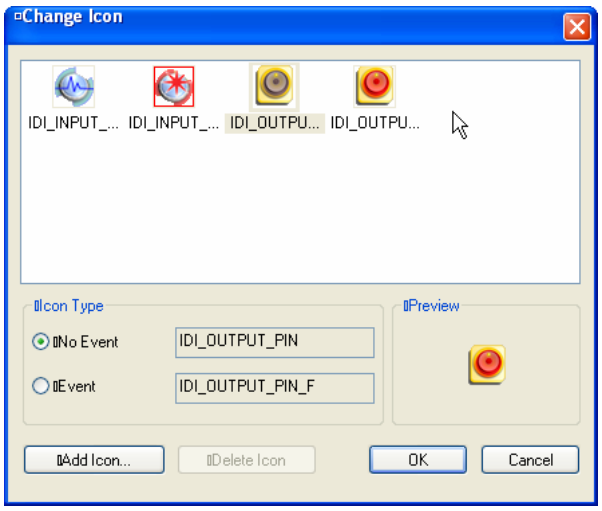


Figure 9.3 *Changing the I/O device icon*

7. Click **File** in the window menu, and select **Save to DVR** or **Save to File** to save the created E-Map file.

9.2.1 Creating an E-Map File for a Remote Host

With E-Map Editor, you can create E-Maps for your local host, as well as remotely for other hosts. E-Maps created for remote hosts are saved at the server where they are created and can only be edited from that server. You have to connect to the E-Maps through the WebCam server to be able to see the live status of the cameras or I/O devices.

Note: The supported host types for E-Map are -DVR/NVR, -IP Devices, -Video Server and -Compact DVR.

---

1. Click the **Add Host** button (No. 3, Figure 9-1) on the toolbar, and select the type of host. A new host is added in Host View.
2. Right-click the created host, and select **Host Settings**. This dialog box appears. The dialog box varies based on the type of host you select.

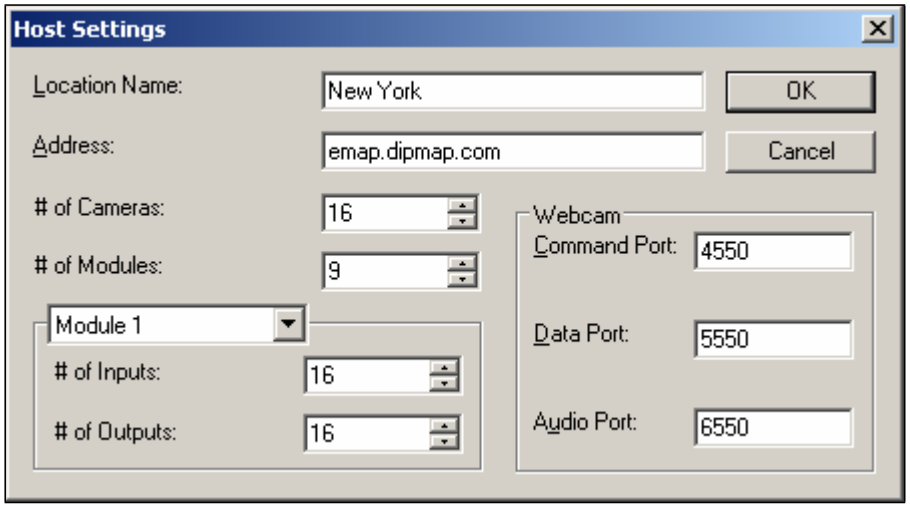


Figure 9-4 *Host Settings*

3. Type the remote host's name, IP address, how many cameras, I/O modules, inputs, outputs are installed at the host, and port information. Then click **OK**.
4. Follow the steps instructed in *Creating an E-Map File* to create an e-map file for the remote host.

9.2.2 Setting Polygonal Map to Locate a Triggered Device

The Polygonal Map function helps you quickly locate the location of a triggered device. Draw an area on the map and it will flash when any device within the area is triggered.

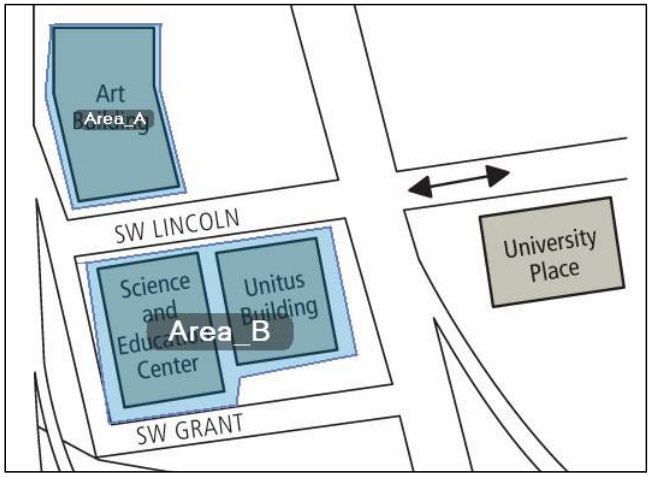


Figure 9-5 *Polygonal Map*

To Set Up a Polygonal Map

1. In E-Map, select a map icon .
2. Right-click the map icon and select **Edit Polygonal Map**.
3. Click on the map to start drawing a polygonal shape, indicated by a yellow dotted line.

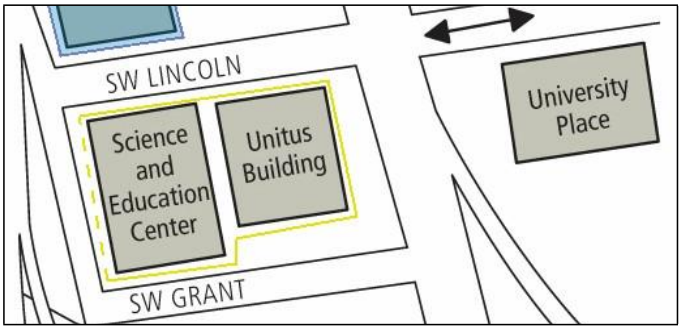


Figure 9-6

4. After closing the shape, right-click the map and select **Finish**.

The enclosed area will be colored in blue. When a device placed within the map is triggered, the blue area will flash in blue and red.

9.2.3 Setting View Zone to Show the Monitored Area

The **View Zone** function allows you to draw an area to represent the area monitored by each device.

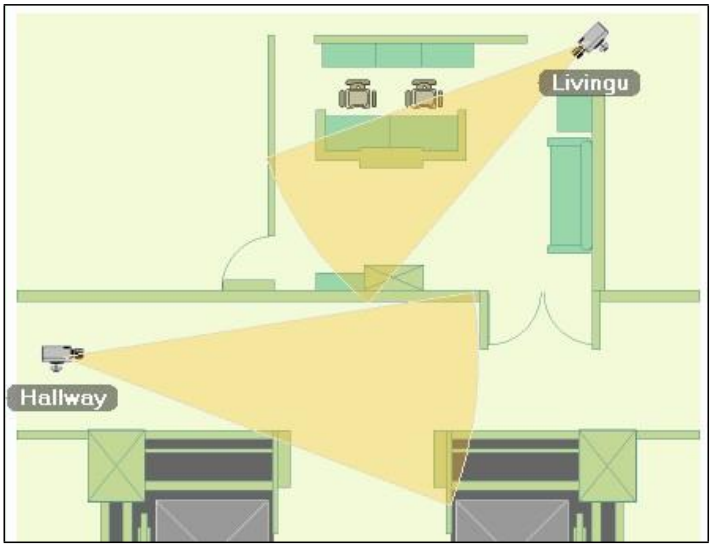


Figure 9-7 *View Zone*

To Set Up a View Zone

1. In E-Map, select a device icon.
2. Right-click the device icon and select **Edit View Zone**.
3. Move the mouse to adjust the length and direction of the view zone.

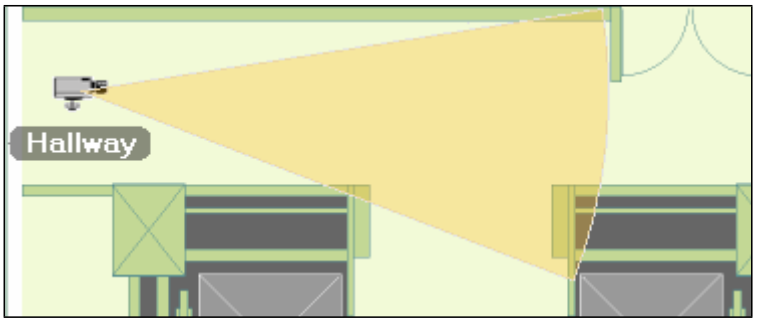


Figure 9-8

4. Scroll the mouse to adjust the width of the view zone.
5. Right-click the map and select **Finish** to finalize the zone.

9.3 Starting E-Map

After creating an E-Map file, go to the Main System. Click the **ViewLog** button (No.13, Figure 1-2) and then select **E-Map** to display the following E-Map Viewer window. Double-click any E-Map file of the local host to open it.

Note: If you have created the E-Map files for remote hosts, these files will also be displayed in the E-Map Viewer window but won't function here. They only work on WebCam that is discussed later.

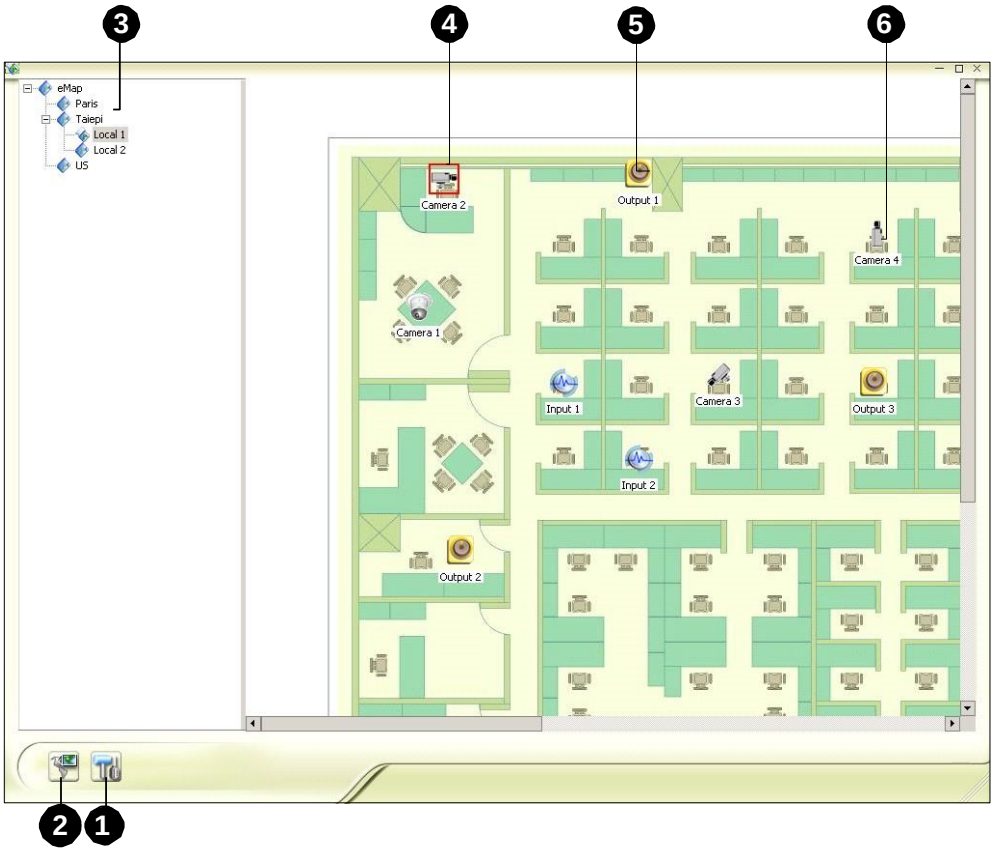


Figure 9-9 *The E-Map Viewer Window*

The controls in the E-Map Viewer window:

No.	Name	Description
1	Popup Settings	Selects desired cameras and I/O devices for the pop-up map function.
2	Toggle Popup	Toggles between popup and non-popup function.
3	Tree View	The tree view of E-Map files and folders.
4	Blinking Icon	The blinking icon represents a triggered camera or an I/O device.
5	Output Icon	Manually forces an output device.
6	Camera/Dome Icon	Views the live video associated with that camera/dome.

9.3.1 Setting the Pop-up Map Function

The E-Map Viewer window can be set to pop up with the blinking icons indicating that cameras or input devices are being triggered. To set up the function, follow the steps below.

1. Click the **Popup Settings** button (No.1, Figure 9-9).
2. Select desired cameras and input devices for the application, and specify **Dwell Time** for the interval between pop-up maps. Any event trigger will be ignored by the system during the interval to avoid map popping up frequently.
3. Click the **Toggle Popup** button (No.2, Figure 9-9) to enable the function.
4. Minimize the E-Map Viewer window. Once any camera or input device is triggered, the map will pop up on your screen immediately.

9.4 Starting E-Map from a Remote Site

Activating and viewing E-Maps over a web browser is possible through the WebCam server. To do so, follow the steps below.

1. At the local server equipped with the -System, click the **Network** button (No. 11, Figure 1-2) and select **WebCam Server** to display the Server Setup dialog box. Click **OK** to start the WebCam server.
2. At the client PC, open the web browser and type the address of the local server. Once the connection is established, the Single View page will appear.
3. On the left panel, click **Remote E-Map** to display the E-Map window on the client PC.

9.4.1 The Remote E-Map Window

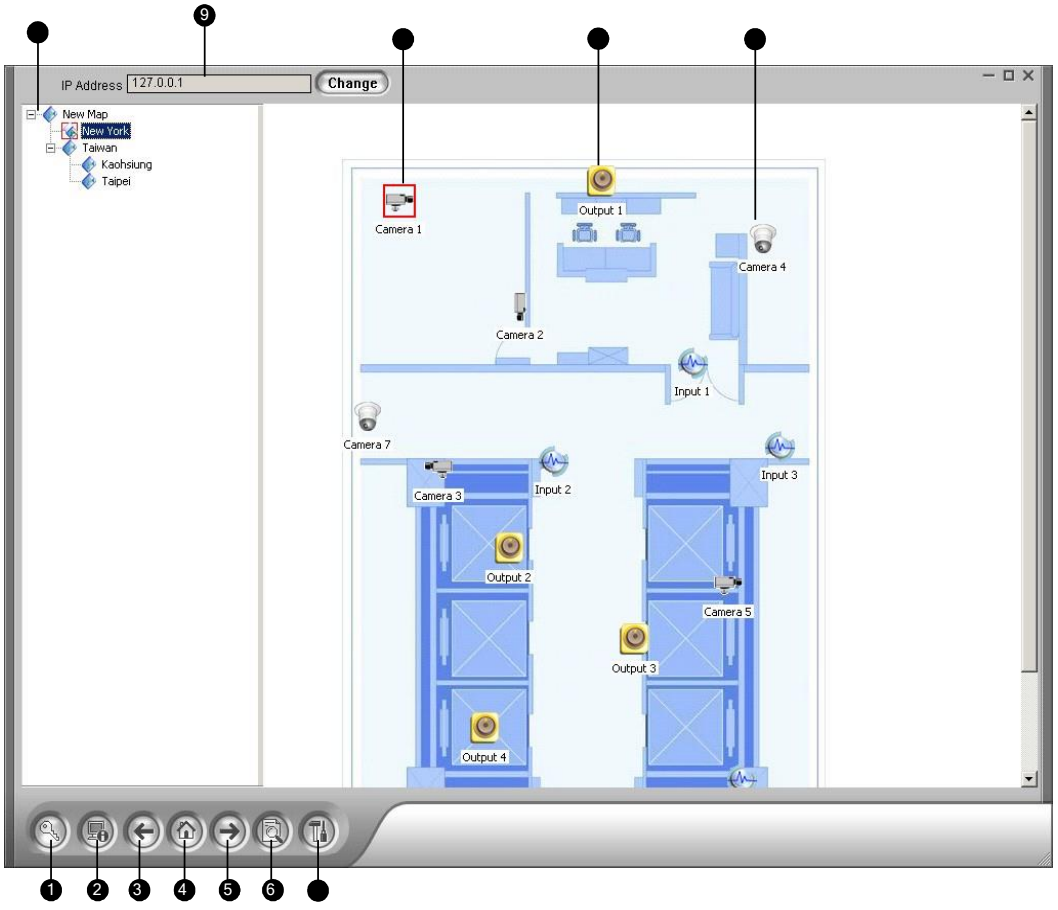


Figure 9-10 *The Remote E-Map Window*

The controls in the Remote E-Map window:

No.	Name	Description
1	Login	Click to login up to 500 hosts.
2	Host Information	Click to view the information of incoming events upon motion detected and I/O devices triggered.
3	Previous	Click to go to the last selected E-Map file.
4	Home	Click to back to the top of the tree view.
5	Next	Click to go to the next E-Map file.
6	ViewLog	Click to access the Remote ViewLog function.
7	Configure	Click to configure the Remote E-Map.
8	Tree List	The list displays all created E-Map files and folders.
9	IP Address	Displays the IP Address of the connected host.
10	Blinking Icon	The blinking icon represents a triggered camera or I/O device.
11	Output Icon	Click to manually force the output device.
12	Camera/Dome Icon	Click to view the live video associated with that camera/dome. Up to 16 live videos can be accessed simultaneously.

9.4.2 Logging in Different Hosts

When the client PC connects to the WebCam server, all the E-Maps saved in the local server will be downloaded to the client PC, with the E-Map files of 500 hosts at most. The E-Maps created for remote hosts can only function through WebCam after you log in these hosts. You can login 500 hosts at a time. Click the **Login** button (No. 1, Figure 9-10) to display the following Login window.

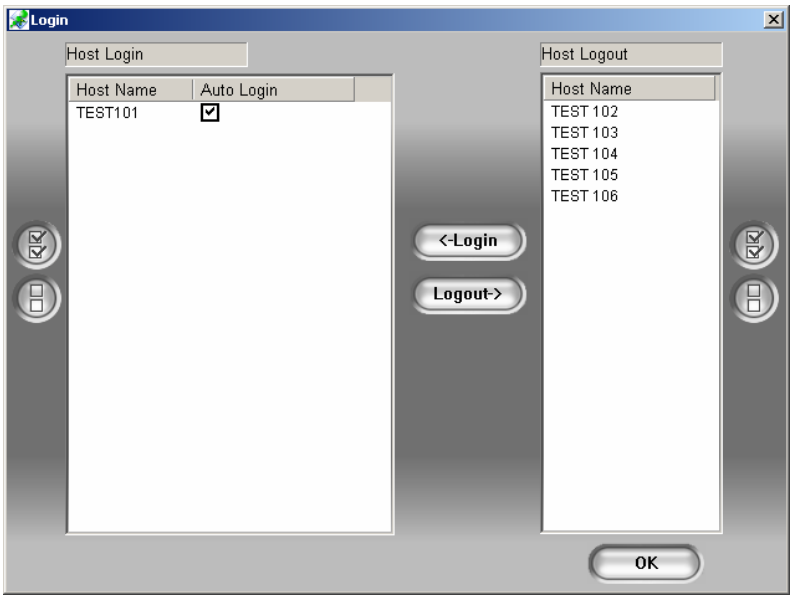


Figure 9-11 *Logging in different hosts*

9.4.3 Configuring the Remote E-Map

Click the **Configure** button (No. 7, Figure 9-10) to display the following dialog box:

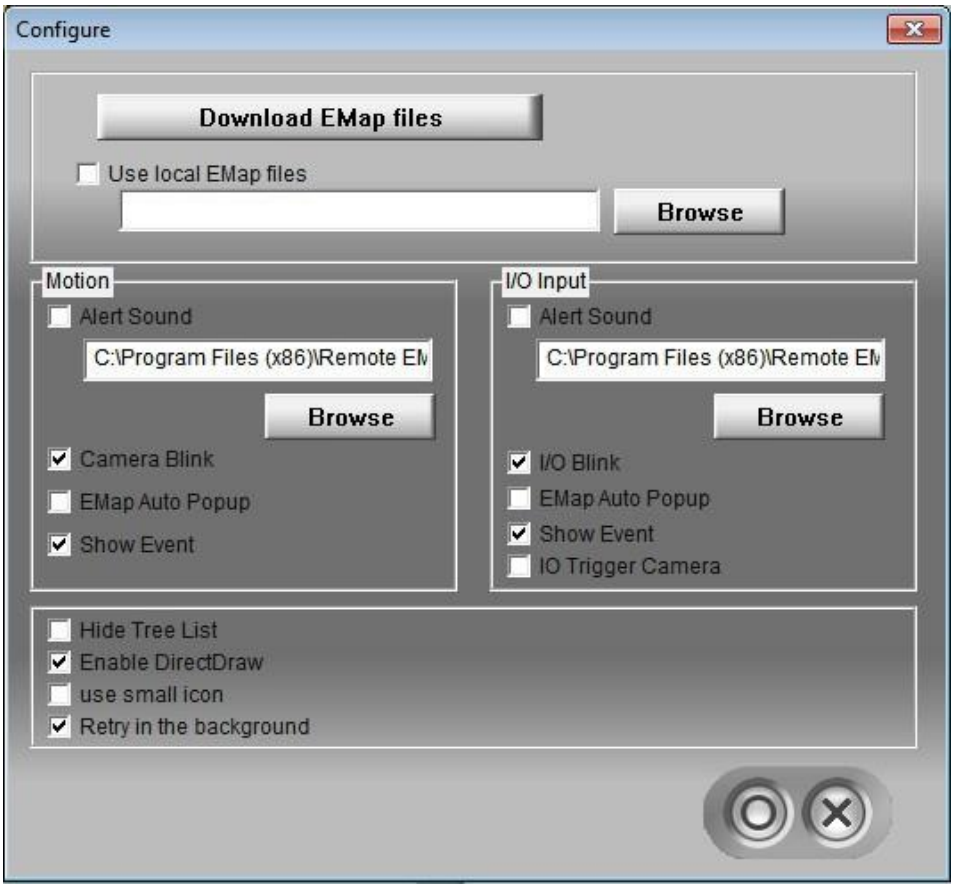


Figure 9-12 *The Configure Dialog Box*

[Download EMap files] Click to download E-Map files from the local server to the client PC. This option can reduce network load when you want to view E-Maps of multiple hosts.

④ **Use local EMap files:** Once downloading E-Map files to the client PC, you can use these E-Map files for connection.

[Motion] / [I/O Input]

④ **Alert Sound:** Check this option and assign a .wav file to alert the operator when motion is detected or I/O devices are triggered.

④ **Camera Blink, I/O Blink:** When cameras or I/O devices are triggered, their icons on the E-map flash. Uncheck this option if you don't want to see the blinking icons.

④ **EMap Auto Popup:** When cameras or I/O devices are triggered, the related map will pop up on the screen instantly. Check this option and minimize the Remote E-Map window for the application.

④ **Show Event:** Check to display motion or I/O triggered events on the Host Information window.

④ **I/O Trigger Camera:** When input devices are triggered, the related camera views will pop up on the screen instantly. For this function to work, input devices must be mapped to cameras on the Main System. See *Pop-up Live View* in Chapter 1.

④ **Hide Tree List:** Check to hide the tree list.

④ **Enable DirectDraw:** The DirectDraw is enabled by default. Some VGA cards might not support DirectDraw and can produce distorted frames. In this case, disable the feature.

④ **Use small icon:** The Remote E-Map uses the large icons of cameras and I/O devices by default. Select this option if you want to use small icons.

④ **Retry in the background:** When Remote E-map is disconnected with the -System, the Remote E-Map will automatically re-connect the -System in 5 seconds. Select this function to avoid the Server Closed message popping up each time the connection failed but the auto-connection still retries in the background.

9.4.4 Viewing Host Information and Playing Back Video

The Host Information window lists the triggered events of cameras and I/O devices. Click the **Host Information** button (No. 2, Figure 9-10) to open it.

The Host Information window allows you to play back events happened in the host sites. Double-click any **Camera Motion** event in the left panel to display the remote playback window. With this window, you can play back an event, speak to the host site and take a snapshot, as well as download the event to the client PC.

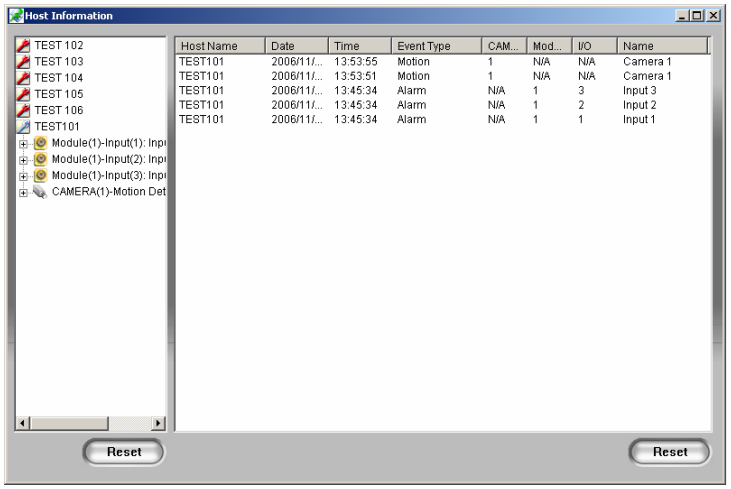


Figure 9-13 *Host Information*

9.4.5 Accessing Remote ViewLog

On the Remote E-Map window, the **ViewLog** button (No.6, Figure 9-10) is designed for the Remote ViewLog function, giving you remote access to the recorded files of DVR and playing back video by the player ViewLog. For details on starting the Remote ViewLog service, refer to *Remote ViewLog* in Chapter 8.

9.5 E-Map Server

The E-Map Server is an independent application, designed to create E-Maps for different DVRs and run without the -System.

9.5.1 Installing E-Map Server

1. Insert the Software DVD to your computer. It will run automatically, and a window appears.
2. Click **Install Sting Alarm Supplemental Utilities**.
3. Click **-E-Map Server**, and then follow the on-screen instructions.

9.5.2 The E-Map Server Window

Go to Windows **Start**, point to **Programs**, select **eMapServer**, and then click **E-Map Server**. This window appears.

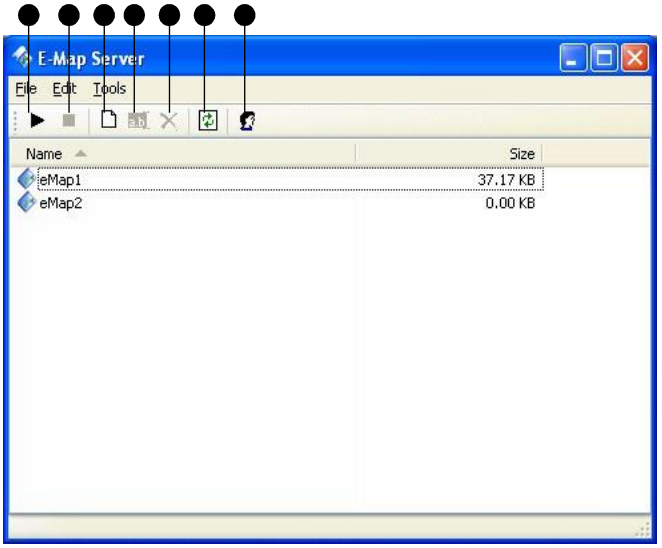


Figure 9-14

The controls on the E-Map Server window:

No.	Name	Description
1	Start Service	Starts the E-Map Server.
2	Stop Service	Stops the E-Map Server.
3	New	Creates a new E-Map file.
4	Rename	Renames the E-Map file.
5	Delete	Deletes the E-Map file.
6	Refresh	Refreshes the E-Map Server window.
7	Accounts	Creates user accounts of the E-Map Server.

9.5.3 Setting E-Map Server

Before starting the E-Map server, you have to create e-map files and user accounts.

1. Click the **New** button (No.3, Figure 9-14) to create e-map(s). For details on creating an e-map file, see *Creating an E-Map File* earlier in this chapter.
2. Click the **Accounts** (No. 7, Figure 9-14) button to create a user account that will use the server.

9.5.4 Remote Monitoring via E-Map Server

Via E-Map Server, you can monitor different surveillance sites on electronic maps from any computer accessible to Internet.

1. Open the web browser and type the address of the E-Map server.
2. After entering the valid user name and password for login, you will be prompted to select the desired e-map file (.emp file),
3. Click **OK**. The Remote E-Map window appears.
4. Click the **Login** button (No.1, Figure 9-10) to select the desired host(s) to access videos and I/O devices.

Note: The host (DVR) needs to give the access privilege by enabling the **WebCam Server**.

9.5.5 Accessing Authentication Server Account Information

With the connection to Authentication Server, the E-Map Server can access the Authentication account settings. For details see *Authentication Server* in Chapter 11.

Chapter 10

Short Message Service 484

10.1 Installing SMS Server 484

10.2 The SMS Server Window 485

10.3 SMS Server Setup 486

10.3.1 Device Settings 486

10.3.2 Server Settings 487

10.3.3 Account Settings 490

10.4 SMS Log 492

10.4.1 Setting SMS Log 492

10.4.2 Viewing SMS Log 493

10.5 Password Security 495

10.6 SMS Notification 495

10.6.1 Connecting -System to SMS Server 495

10.6.2 Setting Mobile Numbers 497

10.6.3 Setting Alert Notification 498

CHAPTER

10

Short Message Service

Via a GSM/GPRS modem, -System lets you send SMS (Short Message Service) messages when an alert condition happens. The modem can be installed at either a separate server, or the same computer/server equipped with -System. This chapter introduces how to manage a GSM/GPRS modem with the -developed SMS Server program, and how to configure the Main System to send out SMS alerts.

For supported GPRS models, see *Appendix F*.

10.1 Installing SMS Server

To install the SMS Server application, follow these steps:

1. Insert the Software DVD to the PC connected to a GSM/GPRS modem. It will run automatically, and a window appears.
2. Click **Install Sting Alarm Supplemental Utilities.**
3. Click **-SMS Server**, and follow the on-screen instructions.

10.2 The SMS Server Window

Run the SMS Server program from the Start menu. The following window appears.

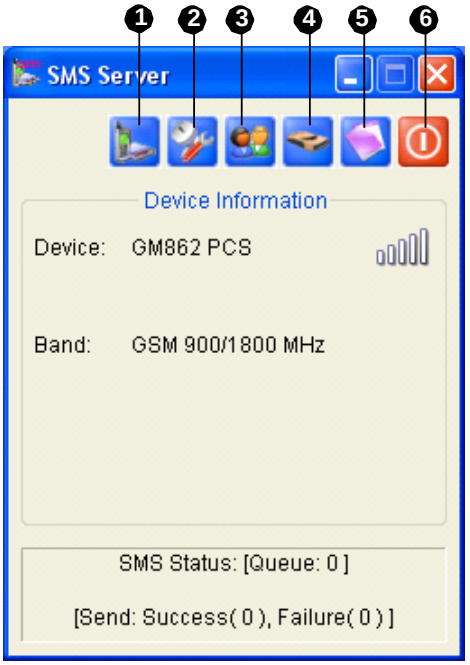


Figure 10-1 *The SMS Server Window*

The controls in the SMS Server window:

No.	Name	Description
1	Start/Stop Service	Starts or stops the SMS Server.
2	Server Setting	Sets up the SMS Server.
3	Account Setting	Creates and edits accounts.
4	SMS Log Setting	Sets up and accesses the SMS Log.
5	Device Setting	Sets up the GSM/GPRS modem.
6	Exit	Logs out administrator, changes password or exits the SMS server.

10.3 SMS Server Setup

Before starting the SMS service, you must configure these three settings: (1) Device Settings, (2) Server Settings, and (3) Account Settings.

10.3.1 Device Settings

1. Click the **Device Setting** button (No. 5, Figure 10-1), and then select **GSM Module**. This dialog box appears.

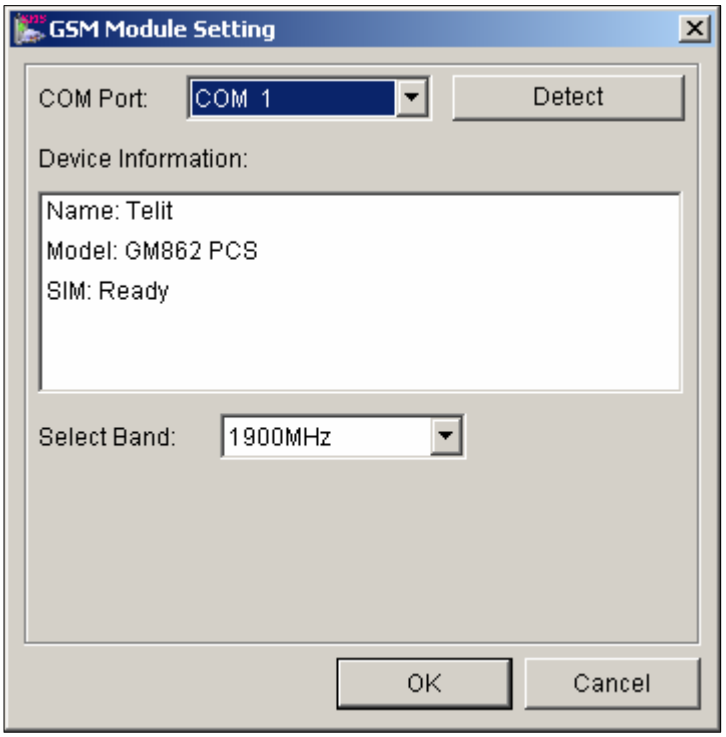


Figure 10-2 *GSM Module Setting*

2. Select the **COM port** connecting to a GSM/GPRS modem.
3. Click the **Detect** button to detect the modem.
   - If the connection between the modem and the computer is established, the message will show in the Device Information field: *Name: (Manufacturer), Module: xxx, SIM Ready.*
   - If the connection fails, the display will be shown as: *No usable device in COM xxx.*
4. If you are using a tri-band modem, select **1900** or **1800 MHz** from the drop-down list of Select Band.
5. Click **OK** to apply above settings.

10.3.2 Server Settings

Click the **Server Setting** button (No. 2, Figure 10-1) to display the following Server Setting dialog box. There are three major tabs in the dialog box: (1) General, (2) Message Filter, and (3) Notify

[General]

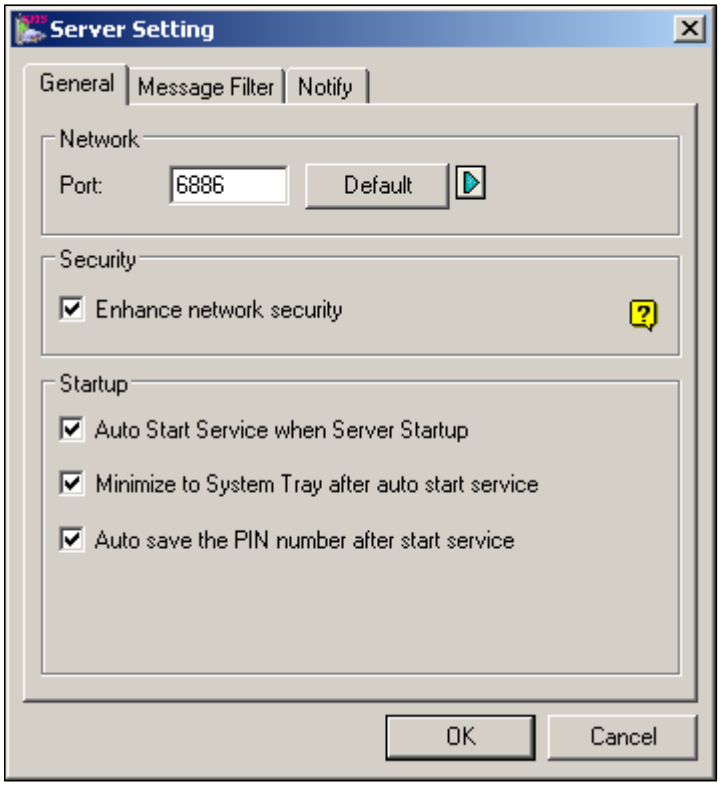


Figure 10-3 *Server Setting-General*

[Network] Define the port of the SMS Server, or leave it as default. To use UPnP for automatic port configuration to your router, click the Arrow button. For details, see *UPnP Settings* in Chapter 8.

[Security] Enable to apply enhanced Internet security. Please note when the feature is enabled, the subscribers using earlier version than 8.0 cannot access the SMS Server anymore.

[Startup]

④ **Auto Start Service when Sever Startup:** Automatically starts SMS services when the program starts.

④ **Minimize to System Tray when auto start service:** Minimizes the SMS Server window to notification area when it starts.

④ **Auto save the PIN number after start service:** Automatically saves the PIN number when SMS services start.

[Message Filter]

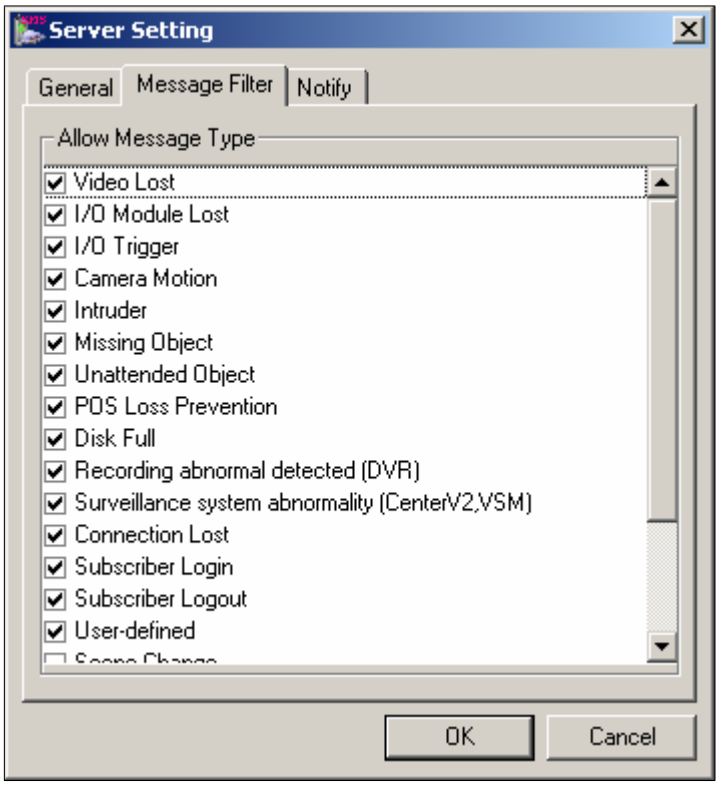


Figure 10-4 *Server Setting-Message Filter*

Check the desired alert conditions to send SMS messages.

The **user-defined** condition refers to the SMS messages sent manually in Center V2 and VSM. See *Sending SMS* in Chapter 1 and Chapter 3 in the *CMS User's Manual*.

[Notify]

Figure 10-5 *Server Setting-Notify*

[Check Internet Connectivity] Assign any available IP address and click the **Test** button to know if your SMS Server can access Internet.

[Send SMS notification when no connectivity] Sends SMS notification to the three designated mobile numbers when the SMS Server cannot access Internet. You can specify the minimum time interval between each notification in minutes.

④ **Mobile Icon:** Check the icon and define the number for the SMS notification. Up to three recipients can receive the SMS simultaneously.

10.3.3 Account Settings

Click the **Account Setting** button (No.3, Figure 10-1) to display the following window.

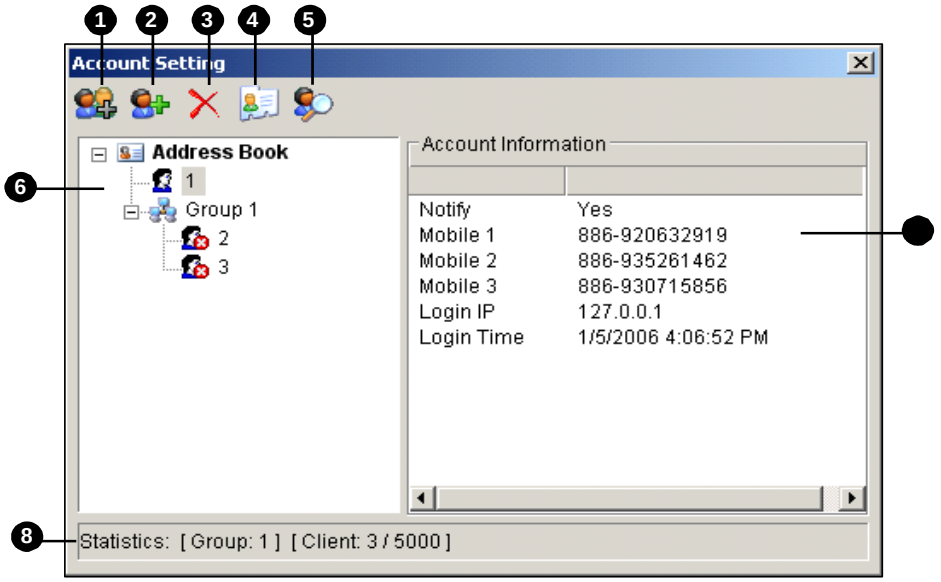


Figure 10-6 *Account Setting*

The controls in the Account Setting window:

No.	Name	Description
1	Add A Group	Creates a group.
2	Add A Client	Creates a client.
3	Delete A Group/Client	Deletes a created group or client.
4	View/Edit A Client	Highlight one client and click the button to view or edit its information.
5	Find A Client	Searches a client.
6	Address Book	Lists the created groups and clients.
7	Account Information	Displays the highlighted client's account information.
8	Statistics	Displays the number of created groups and clients. The SMS Server can serve up to 5000 clients at one time.

Creating a client:

1. Click the **Add A Client** button (No. 2, Figure 10-6). This dialog box appears.

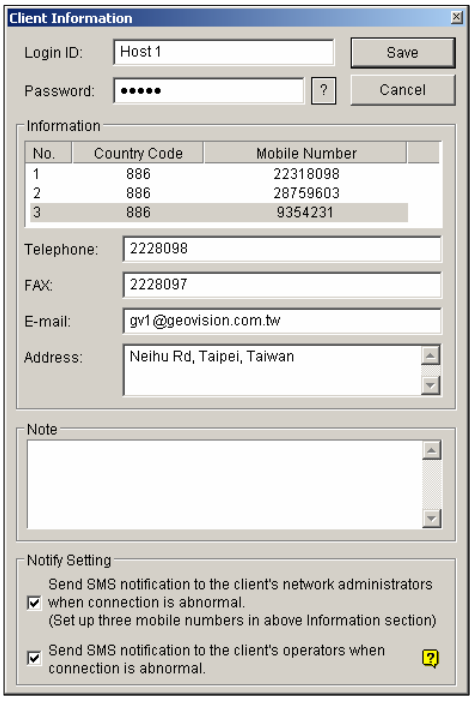


Figure 10-7 *Client Information*

2. Type a login ID and a password. They will be the ID and password for the client to log in the SMS Server (Figure 10-13).
3. In the Information section, type the client's related information.
   You can specify three mobile numbers of the client's network administrators for SMS notification.
4. In the Notify Setting section, you can send a SMS message to the client in the case of:
   - Internet disconnection between the client and the SMS Server, or
   - Improper program shutdown in the client.

   The recipients can be:
   - The client's network administrators: designate three mobile numbers in above Information section.
   - The client's operators: See *Setting Mobile Numbers* later in this chapter. For the users of Dispatch Server and Vital Sign Monitor, refer to the *CMS User's Manual*. Clicking the **Question** mark can view the specified mobile numbers at the client site.
5. Click **Save** for above settings.

Disabling a client:

You can disable subscription services to an individual client when subscription expires.

In the Account Settings window (Figure 10-6), right-click the desired client and then select **Disable**.

To restore the service, right-click the desired client and then select **Enable**.

10.4 SMS Log

10.4.1 Setting SMS Log

Click the **SMS Log Setting** button in the SMS Server window (No. 4, Figure 10-1), and select **SMSLog Setting** to display this dialog box.

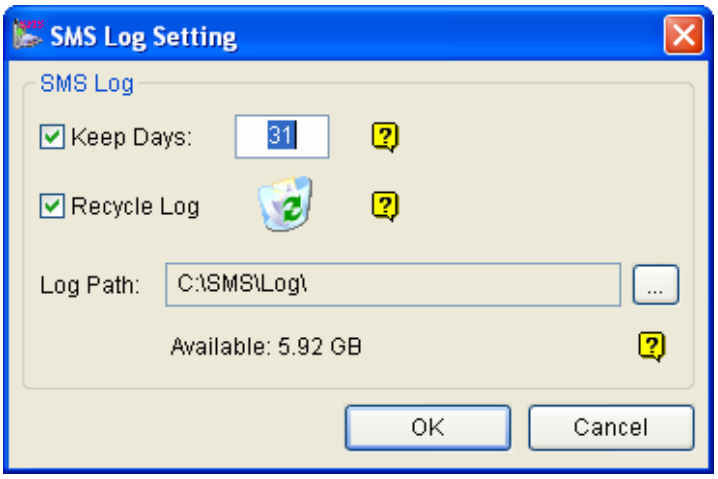


Figure 10-8

[SMS Log]

④ **Keep Days:** Select this option and enter the number of days to keep log files. Otherwise clear the option to keep log files until the Recycle starts or the storage space is full.

④ **Recycle:** Delete the files of the oldest day when storage space is lower than 500MB.

④ **Log Path:** Click the **[...]** button to assign a storage path.

10.4.2 Viewing SMS Log

Click the **SMS Log Setting** button in the SMS Server window (No. 4, Figure 10-1), and select **View SMSLog** to display the SMS Log Browser.

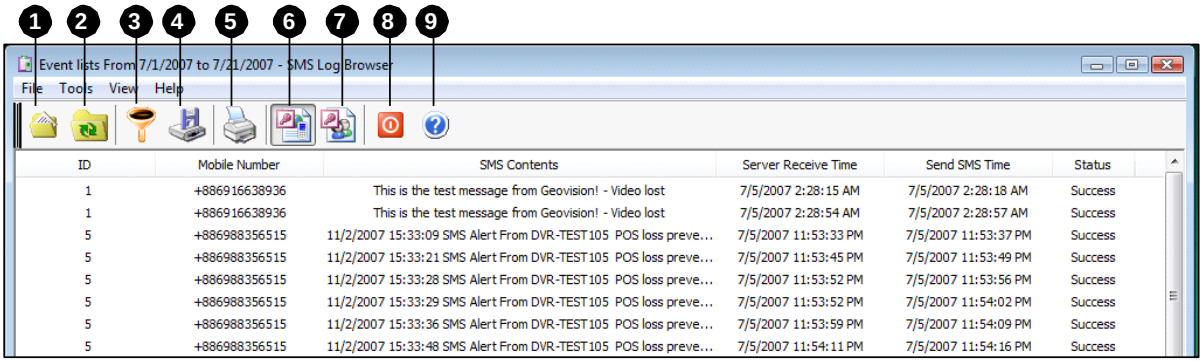

1
2
3
4
5
6
7
8
9
Event lists From 7/1/2007 to 7/21/2007 - SMS Log Browser
File Tools View Help
ID Mobile Number SMS Contents Server Receive Time Send SMS Time Status
1 +886916638936 This is the test message from Geovision! - Video lost 7/5/2007 2:28:15 AM 7/5/2007 2:28:18 AM Success
1 +886916638936 This is the test message from Geovision! - Video lost 7/5/2007 2:28:54 AM 7/5/2007 2:28:57 AM Success
5 +886988356515 11/2/2007 15:33:09 SMS Alert From DVR-TEST105 POS loss preve... 7/5/2007 11:53:33 PM 7/5/2007 11:53:37 PM Success
5 +886988356515 11/2/2007 15:33:21 SMS Alert From DVR-TEST105 POS loss preve... 7/5/2007 11:53:45 PM 7/5/2007 11:53:49 PM Success
5 +886988356515 11/2/2007 15:33:28 SMS Alert From DVR-TEST105 POS loss preve... 7/5/2007 11:53:52 PM 7/5/2007 11:53:56 PM Success
5 +886988356515 11/2/2007 15:33:29 SMS Alert From DVR-TEST105 POS loss preve... 7/5/2007 11:53:52 PM 7/5/2007 11:54:02 PM Success
5 +886988356515 11/2/2007 15:33:36 SMS Alert From DVR-TEST105 POS loss preve... 7/5/2007 11:53:59 PM 7/5/2007 11:54:09 PM Success
5 +886988356515 11/2/2007 15:33:48 SMS Alert From DVR-TEST105 POS loss preve... 7/5/2007 11:54:11 PM 7/5/2007 11:54:16 PM Success

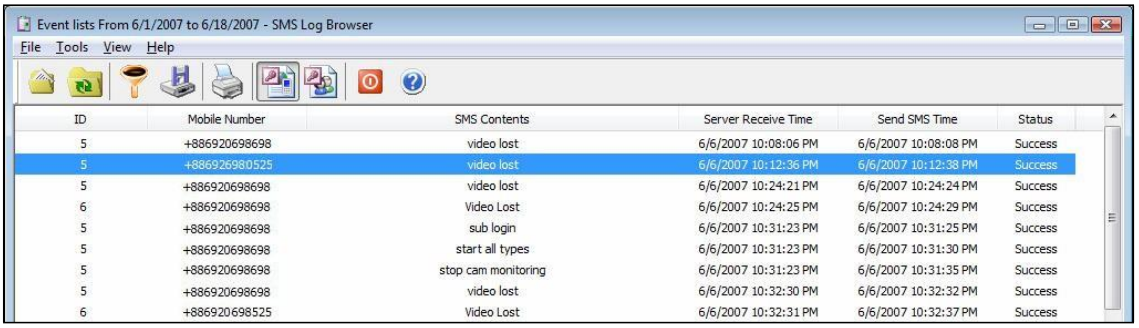
Figure 10-9

The buttons on the Event Log Browser:

No.	Name	Description
1	Open	Opens an event log.
2	Reload	Refreshes the event log manually
3	Filter	Defines the search criteria.
4	Backup	Exports the current event list and video files.
5	Print	Prints the current event list.
6	SMS Event Log	Displays the log of SMS server events.
7	System Event Log	Displays the log of SMS server activities.
8	Exit	Exits the browser.
9	About	Displays the application information of SMS Log Browser.

SMS Event Log

Clicking the **SMS Event Log** button (No. 6, Figure 10-9) on the toolbar, you can monitor senders (ID), mobile numbers, text messages, sent and failed SMS. **This can be beneficial as you may charge your clients by the amount of SMS messages they sent.**



ID	Mobile Number	SMS Contents	Server Receive Time	Send SMS Time	Status
5	+886920698698	video lost	6/6/2007 10:08:06 PM	6/6/2007 10:08:08 PM	Success
5	+886926980525	video lost	6/6/2007 10:12:36 PM	6/6/2007 10:12:38 PM	Success
5	+886920698698	video lost	6/6/2007 10:24:21 PM	6/6/2007 10:24:24 PM	Success
6	+886920698698	Video Lost	6/6/2007 10:24:25 PM	6/6/2007 10:24:29 PM	Success
5	+886920698698	sub login	6/6/2007 10:31:23 PM	6/6/2007 10:31:25 PM	Success
5	+886920698698	start all types	6/6/2007 10:31:23 PM	6/6/2007 10:31:30 PM	Success
5	+886920698698	stop cam monitoring	6/6/2007 10:31:23 PM	6/6/2007 10:31:35 PM	Success
5	+886920698698	video lost	6/6/2007 10:32:30 PM	6/6/2007 10:32:32 PM	Success
6	+886920698525	Video Lost	6/6/2007 10:32:31 PM	6/6/2007 10:32:37 PM	Success

Figure 10-10

System Event Log

Clicking the **System Event Log** button (No. 7, Figure 10-9) on the toolbar, you can monitor the server activities, client login and logout, and connection problems.

ID	Type	Message	Message Time
System	System	Success to get device (GM862 PCS) in COM2	6/6/2007 12:57:19 AM
System	System	Change server setting (Server Setting)	6/6/2007 12:57:56 AM
System	System	Start Service	6/6/2007 12:58:02 AM
System	Connection	The network connection of server is abnormal	6/6/2007 12:59:12 AM
1	Login/Logout	1 (IP:221.169.248.174) login	6/6/2007 12:59:37 AM
2	Login/Logout	2 (IP:221.169.248.174) login	6/6/2007 1:01:37 AM
2	Login/Logout	This account has already logged in	6/6/2007 1:47:31 AM

Figure 10-11

10.5 Password Security

To prevent unauthorized users from changing your settings, set up an administrator password. To apply the password security, follow these steps:

1. Click the **Exit** button (No. 6, Figure 10-1), and then select **Change Password** to set a password.
2. Click the **Exit** button, and select **Logout Administrator** to lock the SMS Server window.
3. When you want to log in, click the **Exit** button and select **Login as Administrator**. A valid password is required.

10.6 SMS Notification

After setting up the SMS Server, you will need to connect the -System to the SMS Server, assign mobile phones to receive SMS alert messages, and set up the types of events to send alert notification.

10.6.1 Connecting -System to SMS Server

To connect the -System to the SMS Server, follow these steps:

1. On the main screen, click the **Configure** button (No. 14, Figure 1-2), select **System Configure**, and select **Send Alerts Approach Setup**. This dialog box appears.

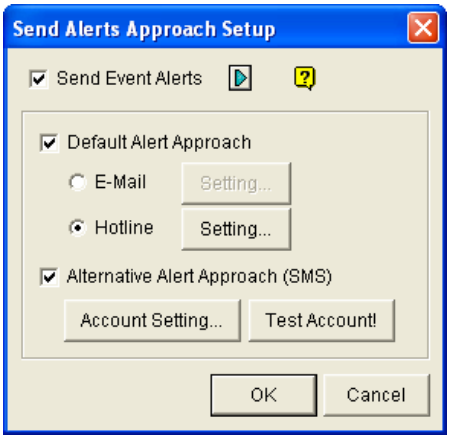


Figure 10-12 *Send Alerts Approach Setup*

2. Select **Send Event Alerts**, click the Arrow button and select the events to send alert notification.
3. Select **Alternative Alert Approach** to enable sending alerts by SMS messages.

4. Click the **Account Setting** button. This dialog box appears.

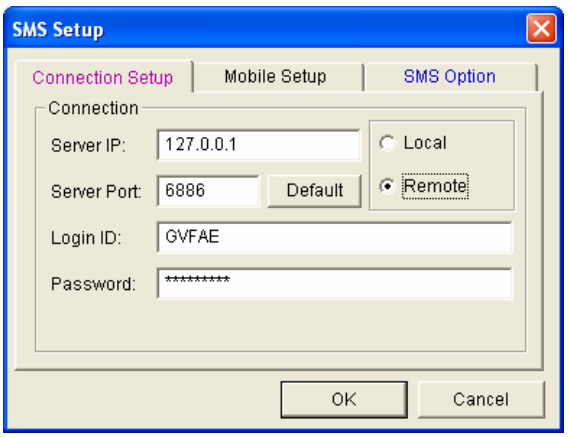


Figure 10-13 *SMS Setup-Connection Setup*

④ **Server IP:** Type the IP address of the SMS Server.

④ **Server Port:** Type the server port of the SMS Server, or keep it as default.

④ **Login ID & Password:** Type a valid ID and password registered in the SMS Server (Figure 10-7).

④ **Local:** If the GSM/GPRS modem is installed at the same server with the -System, select this item.

④ **Remote:** If the GSM/GPRS modem is installed at a separate server, select this item.

5. Click the **SMS Option** tab and specify the Interval between two sent-out messages. The Interval time can be set up to 1440 minutes. Any alert condition will be ignored by the system during the interval.
6. Click **OK** to apply above settings.
7. Click the **Test Account** button (Figure 10-12). If the connection of both devices is established, the message will appear: *Login SMS Server OK!* If the connection fails, the message will appear: *Connect to SMS Server Fail*.

10.6.2 Setting Mobile Numbers

The Main System allows you to configure three mobile phone numbers for the SMS service. When an alert condition happens, the SMS messages will be sent out to the three assigned mobile phones simultaneously.

1. Open the **Send Alerts Approach Setup** dialog box (Figure 10-12).
2. Click the **Account Setting** button. The SMS Setup dialog box appears. (Figure 10-13).
3. Click the **Mobile Setup** tab in the upper of the window. This dialog box appears.

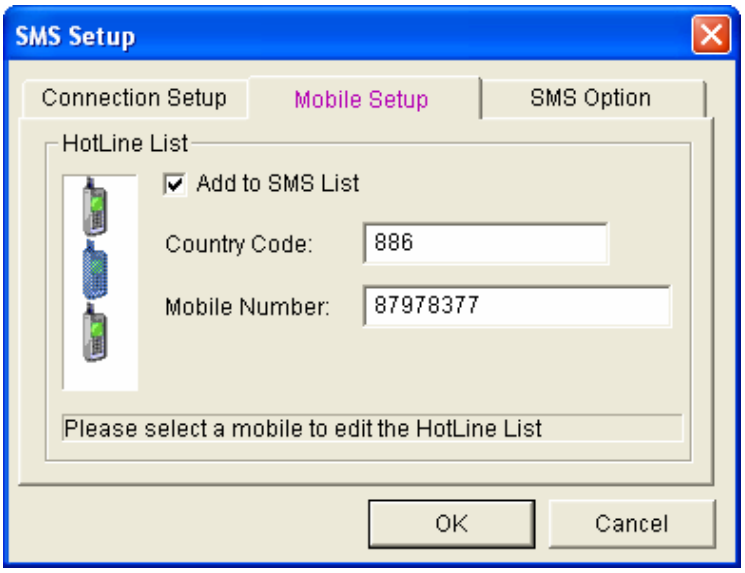


Figure 10-14 *SMS Setup- Mobile Setup*

4. Click one mobile phone icon, and then check the **Add to SMS List** item for the mobile phone setup.
5. Type the **Country Code** and **Mobile Number**.
6. Click other mobile phone icons, and follow Steps 4 and 5 to set up the rest of two mobile phone numbers separately.
7. Click **OK** to apply above settings.
8. Start monitoring. When the specified events or motion is detected, SMS alerts will be sent out automatically.

10.6.3 Setting Alert Notification

To specify the types of events to receive alert notification:

1. On the main screen, click the **Configure** button (No. 14, Figure 1-2), select **System Configure**, and select **Send Alerts Approach Setup**. The Send Alerts Approach Setup dialog box (Figure 10-12) appears.
2. Select **Send Event Alerts**, click the Arrow button and select the events to send alert notification.
3. Click **OK**.

To send SMS alerts when motion is detected:

1. Click the **Configure** button (No.14, Figure 1-2), select **System Configure** and select **Camera Configure**. The Camera Configure dialog box appears.
2. In the Motion Detection section, select **Invoke to Send Alerts**.

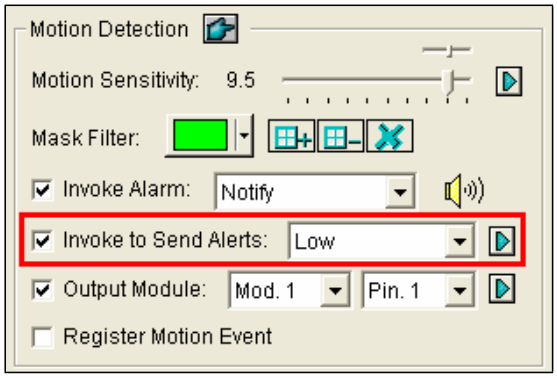


Figure 10-15

3. Click **OK**.

For details on the Invoke to Send Alerts options, see *Invoke to Send Alerts* in Chapter 1.

Chapter 11

Useful Utilities..... 502

11.1 Dynamic DNS 502

11.1.1 Installing Dynamic DNS..... 503

11.1.2 Registering Domain Name with DDNS 504

11.1.3 Starting Dynamic DNS 506

11.1.4 Local DDNS Server 508

11.2 Watermark Viewer 509

11.2.1 Activating Watermark Protection 509

11.2.2 Running the Watermark Proof..... 510

11.2.3 The Watermark Proof Window 511

11.3 Twin View Display 512

11.4 Windows Lockup 514

11.4.1 The -Desktop Screen 514

11.4.2 -Desktop Features..... 515

11.4.3 Token File for Save Mode 518

11.5 Authentication Server..... 519

11.5.1 Installing the Server..... 519

11.5.2 The Server Window..... 520

11.5.3 Creating a Client DVR..... 521

11.5.4 Creating a User Account 522

11.5.5 Importing Groups and Users from Active Directory..... 523

11.5.6 Starting the Server..... 525

11.5.7 Connecting -System to the Server 527

11.5.8 Remote Access from Control Center, Remote E-Map and MultiView 530

11.6 Fast Backup and Restore 533

11.6.1 Installing the FBR Program 533

11.6.2 Customizing Logo and Button 534

11.6.3 Customizing the Features 535

11.6.4 Backing up and Restoring Settings 536

11.7 Hot-Swap Recording..... 538

11.7.1 The Media Man Tool Window..... 539

11.7.2 Viewing Disk Drive Status 540

11.7.3 Adding a Disk Drive..... 542

11.7.4 Removing a Disk Drive 543
11.7.5 Logging In Automatically at Startup 544
11.7.6 Setting LED Panel 545
11.8 Backup Server 547
11.8.1 Adding a Disk Volume 547
11.8.2 Enabling Backup Server 549
11.8.3 Advanced Settings 550
11.8.4 Manually Adding Files for Backup 553
11.8.5 Viewing Server Status 554
11.8.6 Retrieving Recorded Files 556
11.8.7 Viewing Backup Status 557
11.9 Backup Viewer 558
11.9.1 Usage Requirements 558
11.9.2 Starting Backup Viewer 559
11.9.3 Performing Queries 560
11.9.4 Viewing the Event Files 561
11.9.5 Using Remote ViewLog 562
11.10 Bandwidth Control Application 563
11.10.1 Installing the Bandwidth Control 564
11.10.2 Allowing Remote Control at DVR 565
11.10.3 Connecting to a WebCam Server 566
11.10.4 Controlling a WebCam Server 567
11.10.5 Bandwidth Setup 568
11.10.6 Block List Setup 569
11.10.7 General Setup 570
11.11 Report Generator 571
11.11.1 Starting Report Generator 571
11.11.2 Setting Report Generator 572
11.11.3 Setting Report Criteria 574
11.11.4 E-Mail Attachment Settings 577
11.11.5 Playing Back Video Recordings 578
11.11.6 Viewing Event Log 580
11.12 Spot Monitor Controller 581
11.12.1 Spot Monitor Controller 581
11.12.2 Spot Monitor Panel 584

11.13 Quad Spot Monitor Controller 585
11.13.1 Setting the Controller 585
11.13.2 Setting Pop-up Views 588
11.13.3 Displaying TV Quad Panel 589
11.14 Digital Matrix 590
11.14.1 Activating Multiple Monitors 590
11.14.2 Setting Live View 592
11.14.3 Setting Scanned Pages 593
11.14.4 Setting Pop-up Alert 594
11.14.5 Setting Live View with Pop-up Alert 596
11.14.6 Controlling Screen Display 597
11.15 GIS Recording 598
11.15.1 Setting the GPS Receiver 598
11.15.2 Recording GPS Locations of -System 600
11.15.3 Recording GPS Locations of the IP Device 601
11.15.4 Viewing GPS Locations during Playback 602
11.15.5 Sending GPS Data to the -GIS 604
11.16 -IP Device Utility 607
11.16.1 Installing -IP Device Utility 607
11.16.2 The -IP Device Utility Window 608
11.16.3 Setting IP Devices 609
11.16.4 Mapping IP Cameras 610
11.17 MCamCtrl Utility for -Joystick 611
11.17.1 Installing MCamCtrl Utility 611
11.17.2 Starting the MCamCtrl Utility 612
11.18 -Mobile Server 613
11.19 Language Setting 614
11.19.1 MultiLang Tool for Translated Text 614
11.19.2 SetLanguage Tool to Set UI Language 618
11.20 Skype Video Utility 619
11.20.1 Installing -Skype Video Utility 620
11.20.2 Setting Up Notifications Upon Motion or I/O Trigger 621

CHAPTER

11

Useful Utilities

This chapter discusses some advanced features and utilities that could help the administrator to maximize system performance in a security network.

11.1 Dynamic DNS

The Dynamic DNS is an application that allows you to register domain names that always point to your -Systems. This application is only necessary when your -System is using a dynamic IP address. The DDNS will update -System's IP address to DNS Server every 10 minutes. Therefore, even if your -System's IP address changes, you can still locate it by using the registered domain name.

Note:

1. Dynamic DNS uploads IP addresses over the Internet through ports 80 and 81. If your -System is connected behind a router or firewall, make sure ports 80 and 81 are enabled. Dynamic DNS will only upload global IP addresses. If your -System is using virtual IP, NAT port mapping should be done first.
2. Dynamic DNS does not support Windows 95, Windows 98 and ME.

IMPORTANT: The DDNS service is provided purely as a favor to you. We hope it simplifies the process of trying to connect an IP video device to the network. Sting Alarm does not and cannot warrant that the DDNS service will be uninterrupted or error free. Please read Terms of Service carefully before using the service. Besides Sting Alarm, you can also obtain the free DDNS service from these providers: DynDNS.org and No-IP.com.

11.1.1 Installing Dynamic DNS

To install Dynamic DNS, follow these steps:

1. Insert the Software DVD to your computer. It runs automatically, and a window appears.
2. Click **Install Sting Alarm Supplemental Utilities**.
3. Select **-Dynamic DNS Service**, and follow the on-screen instructions.

11.1.2 Registering Domain Name with DDNS

1. Go to Windows **Start**, point to **Programs**, select **DDNS**, and then run **Dynamic DNS Service**. The DNS Client dialog box (Figure 11-3) appears.
2. Click **Register**. The following Dynamic DNS register page appears.
3. Type a username. The username can be up to 16 characters. The username accepts “a ~ z”, “0~9”, and “-“, but does not accept space or “-“ as the first character.
4. Type a password. The password is case-sensitive and must be at least 6 characters. Re-type the password for confirmation.
5. In the Word Verification section, type the code within the box. In this example, the code you should enter is *4NCXRC*. Word verification is not case-sensitive.

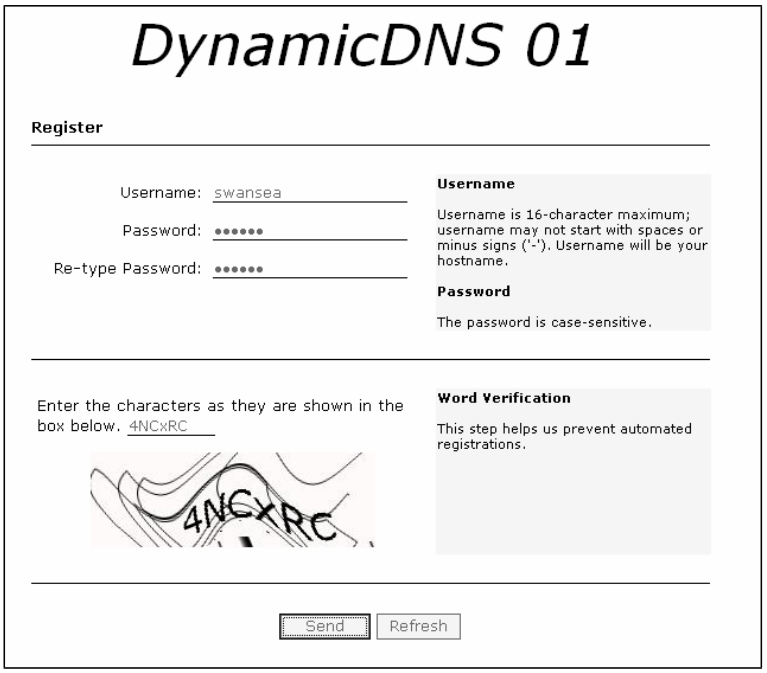


Figure 11-1

6. Click the **Send** button. The following message appears.

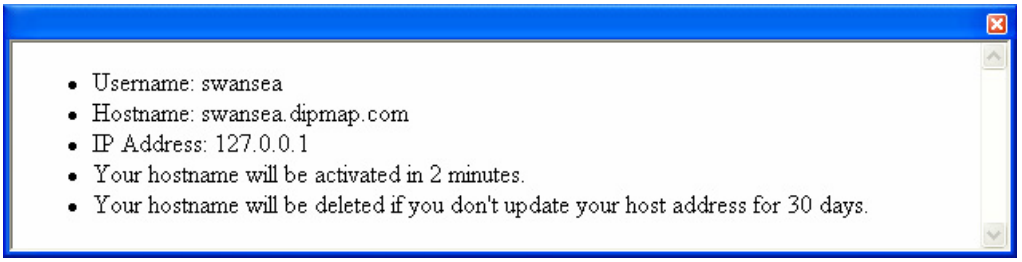

Username: swansea
Hostname: swansea.dipmap.com
IP Address: 127.0.0.1
Your hostname will be activated in 2 minutes.
Your hostname will be deleted if you don't update your host address for 30 days.

Figure 11-2

④ **Username:** The username you registered. In this example the username is “swansea”

④ **Hostname:** The hostname you created. Hostname is made by registered username and “dipmap.com”. In this example the host name is “http://swansea.dipmap.com”. This will be the domain name you use to log into -System.

④ **IP Address:** Your -System’s current IP address. This IP address is updated every 10 minutes.

Note: Before you can register a domain name with Dynamic DNS Service provided by Sting Alarm, it is required to run any Sting Alarm application in the background if the installed -System is of version 8.2 or later.

11.1.3 Starting Dynamic DNS

After registering a domain name with DDNS service, you can enable the DDNS function on the -System. Run **Dynamic DNS Service** from the Windows Start menu. This DNS Client dialog box will appear.

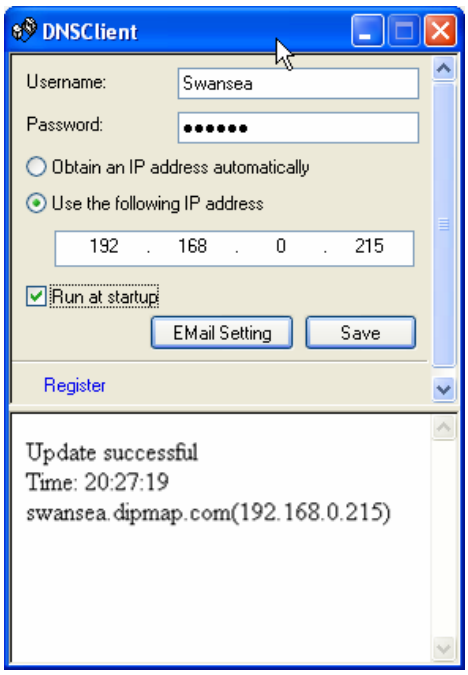


Figure 11-3

④ **Username:** Type the username used to enable the service from the DDNS.

④ **Password:** Type the password used to enable the service from the DDNS.

④ **Obtain an IP address automatically:** The DDNS server will use any available IP address from the system or the router.

④ **Use the following IP address:** If your system or router has more one IP address, you can assign one IP address for the communication between the DDNS server and -System. It is highly suggested to assign the fixed IP address. If the assigned IP address is dynamic, the DDNS will not be able to access your system when the IP address is changed.

④ **Run at startup:** Select this option to automatically run the DDNS service at Windows startup.

④ **Save:** After above settings, click this button. The connection information will be displayed.

Note: The DNS Client will not upload IP address unless one of the following applications is running: Main System, Center V2, VSM, Dispatch Server and SMS Server. If the IP address of your -System is not updated for more than 30 days, your host name will be deleted automatically.

Setting up E-mail Notification

You can set up E-mail settings to receive e-mail notification. In the DNS Client dialog box (Figure 11-3), click **E-mail Setting**. The E-mail Setting dialog box appears.

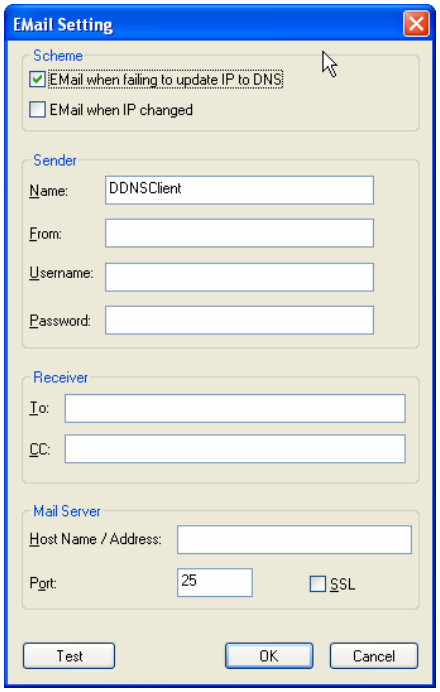


Figure 11-4

[Scheme] Select to receive e-mail notification when failed to update IP to DNS or when IP has changed.

[Sender] Type a name to identify the sender and then type the sender's e-mail address. Type the username and password of mail server.

[Receiver] Type the recipients' e-mail addresses. For multiple recipients, add a semicolon between each e-mail address.

[Mail Server] Type the host name or address of your mail server. You can keep the default port 25 or type your own if the mail server uses a different port. Select **SSL** if your e-mail server requires the SSL authentication for connection.

Click the **Test** button to send a test e-mail and see whether the setup is correct.

11.1.4 Local DDNS Server

The Local DDNS Server can map a device name to the POS device and the AS200E Controller with a dynamic IP, by which the -System can access the POS device and the AS200E Controller by the device name. For details see *-Data Capture V3 Series User's Manual* or *-AS200 Controller Hardware Installation Guide*.

11.2 Watermark Viewer

The -System can embed digital watermarks in video streams for the purpose of authentication. The watermarks are encrypted and digital signatures embedded in video streams during the compression stage, protecting videos from the moment of creation. Watermarking ensures that images are not edited or damaged after they are recorded.

The **Watermark Proof** is a watermark-checking program. It can verify the authenticity of the recording before you present it in court.

11.2.1 Activating Watermark Protection

Click the **Configure** button on the main screen, click **System Configure**, click **General Setting** and select **Use Digital Watermark Protection**. The -System will digitally sign videos as they are recorded.

11.2.2 Running the Watermark Proof

1. Go to the folder, and run **WMProof.exe**.

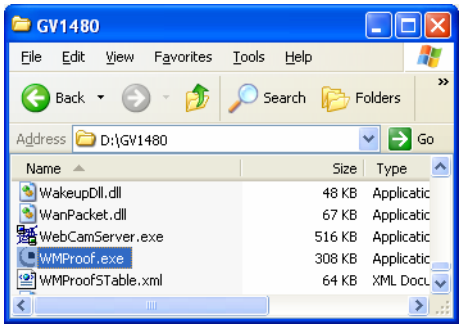


Figure 11-5

2. In the Watermark Proof window, click **File** from the menu bar, select **Open** and locate the recorded file (.avi). The selected file is then listed on the window. Alternatively, you can drag the file directly from the storage folder to the window.
3. If the recording is unmodified, a check mark will appear in the **Pass** column. On the contrary, if the recording is modified or does not contain watermark during recording, a check mark will appear in the **Failed** column. To play the recording, double-click the listed file on the window.

11.2.3 The Watermark Proof Window

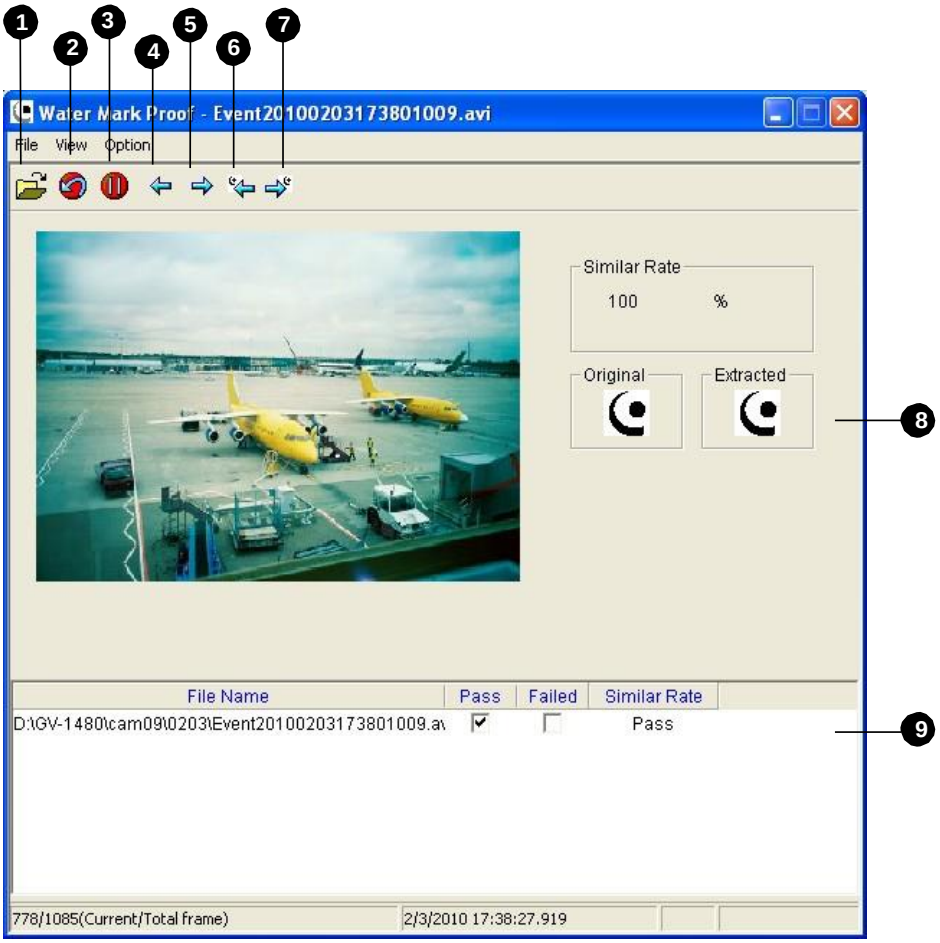


Figure 11-6

The controls in the window:

No.	Name	Description
1	Open File	Opens the recorded file.
2	First Frame	Goes to the first frame of the file.
3	Play	Plays the file.
4	Previous Frame	Goes to the previous frame of the file.
5	Next Frame	Goes to the next frame of the file.
6	Previous Watermarked Frame	Goes to the previous frame that contains watermark.
7	Next Watermarked Frame	Goes to the next frame that contains watermark.
8	Original vs. Extracted	The Extracted icon should be identical with the Original icon. If not, it indicates the recording has been tampered.
9	File List	Displays the proof results.

11.3 Twin View Display

The -System supports dual monitor display, one for live viewing and the other for playback or other operation without obstructing surveillance scene. To make this operation possible, your system must have a graphic card with dual video outputs, and each output should be connected to its own monitor for display.

1. To configure two-monitor display on Windows, right-click on the Windows desktop and select **Properties**. The Display Property dialog box appears.
2. Select **Settings**, enable **Extend my Windows desktop onto this Monitor**, and click the **Apply** button.

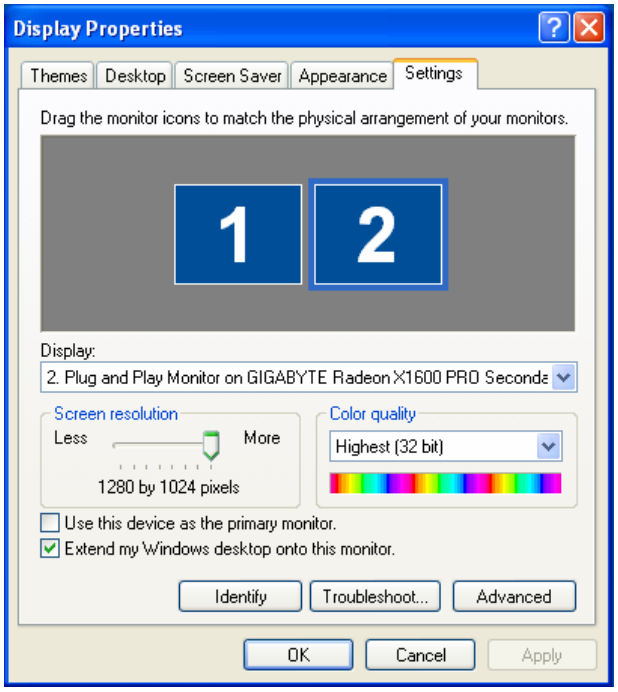


Figure 11-7

3. Go the folder and locate **DMPOS.exe**.

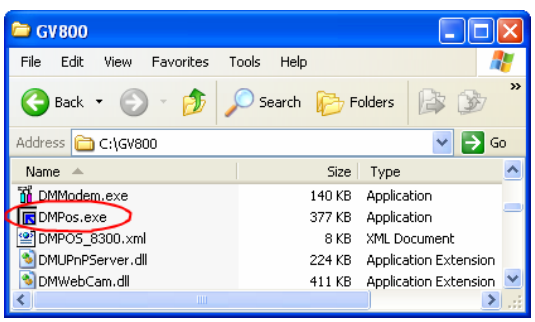


Figure 11-8

4. Run **DMPOS. exe**. This dialog box appears.

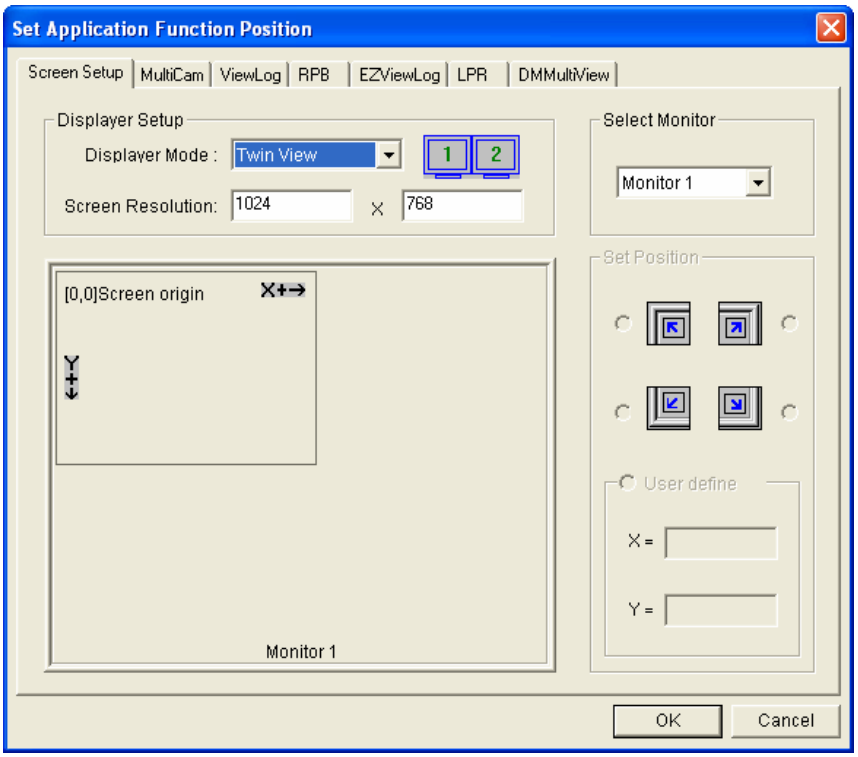


Figure 11-9

5. In the Screen Setup tab, select **Twin View** from the Displayer Mode drop-down list.
6. Click the desired application tab to move the application to the second monitor. In this case, ViewLog is used as an example.
7. In the ViewLog tab, select **Monitor 2** from the Select Monitor drop-down list.
8. Click **OK**.
9. Start -System. It should appear on Monitor 1.
10. Click the **ViewLog** button on the main screen and select **Video/Audio log** from the menu. ViewLog should appear on Monitor 2.

Note: The **Set Position** option allows you to determine where to position -System on Windows. It is only necessary if your -System is set to 800 x 600 panel resolutions but your Windows desktop is set to 1024 x 768 or higher. It is recommended that both -System and Windows desktop to be set to the same resolution. To set the panel resolution of -System, click **Configure** button, select **General Setting**, select **System Configure** and find **Panel Resolution**.

11.4 Windows Lockup

This feature helps you to secure your PC while away from your workstation. You may lock up the Windows desktop while launching a customized -Desktop. The -Desktop is where operators are limited to run the -System and the selected programs.

11.4.1 The -Desktop Screen

The -Desktop program is included in the installation of Main System. Go to Windows **Start**, point to **Programs**, select folder, and click **Key Lock Utility**. This -Desktop screen appears.

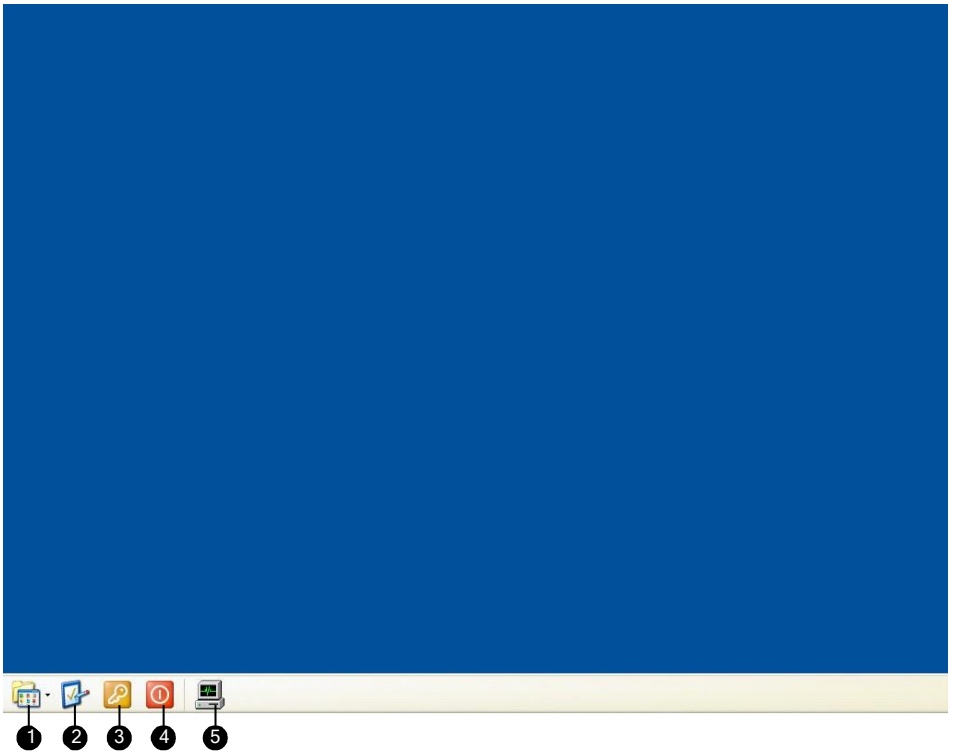


Figure 11-10

The controls in the -Desktop screen:

No.	Name	Description
1	Programs	Accesses programs.
2	Settings	Adds programs to the programs menu.
3	Log Off	Logs off -Desktop.
4	Shut Down	Shuts down the computer.
5	Task Manager	Click to view the tasks currently running on your computer.

11.4.2 -Desktop Features

The five buttons on -Desktop are discussed below.

Programs

Click the **Programs** button (No.1, Figure 11-10) to see the program menu. The default programs are Multicam Surveillance System (Main System), ViewLog, Repair Database Utility, eMap Editor, Control Center Service and Hot Swap HDD Tool. You can add or remove new programs to the menu. In the example below, Paint is a new program added to the menu.

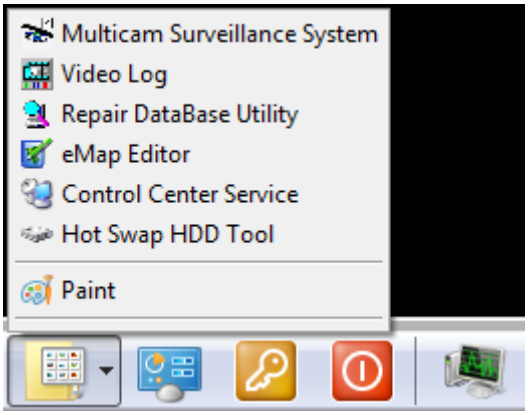


Figure 11-11

Settings

Click the **Settings** button (No.2, Figure 11-10) to display the following window. A valid ID and password are required.

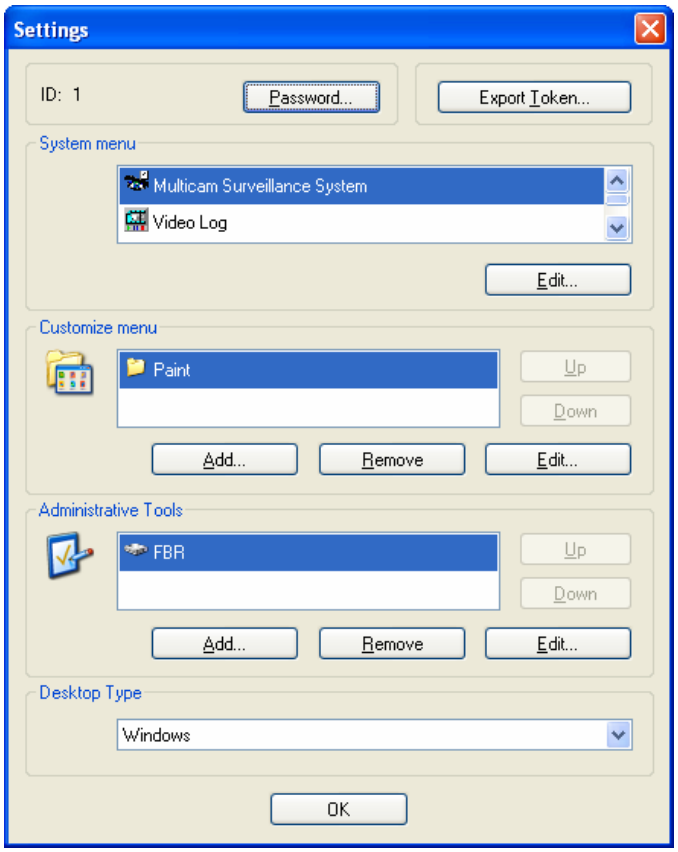


Figure 11-12

[Password] Click to change the password. For the **Allow Removing Password System** option, see *Account and Password* in Chapter 1.

[Export Token] This option is discussed in *Token File for Save Mode* later in this chapter.

[System Menu] The menu lets you rename system programs. Select a desired program and click the **Edit** button to change its name.

[Customized Menu] The menu lets you add other programs to the Programs menu. Click the **Add** button. The Shortcut dialog box will appear. In the Target field, type a path or click the button next to the field to assign a path. Then enter the program name, comment, or even change an icon for the program. Finally, click **OK** to add the program.

[Administrative Tools] Similar to Customized Menu, the option lets you add other programs to the Programs menu. But when you want to run the added program, the administrative ID and Password are required.

[Desktop Type] Select Windows or -Desktop (Multicam) from the drop-down menu. The selected desktop will launch the next time when you log in to PC.

Log Off

Click the **Log off** button (No.3, Figure 11-10) to log off -Desktop. A valid ID and password are required.

Shut Down

Click the **Shut Down** button (No. 4, Figure 11-10) to shut down your computer. A valid ID and password are required.

Task Manager

Click the **Task Manager** button (No. 5, Figure 11-10) to view the programs currently running on your computer. When you minimize a program, it will be hiding and working in the background. Double-click the program listed in Task Manager to bring the program back to desktop.

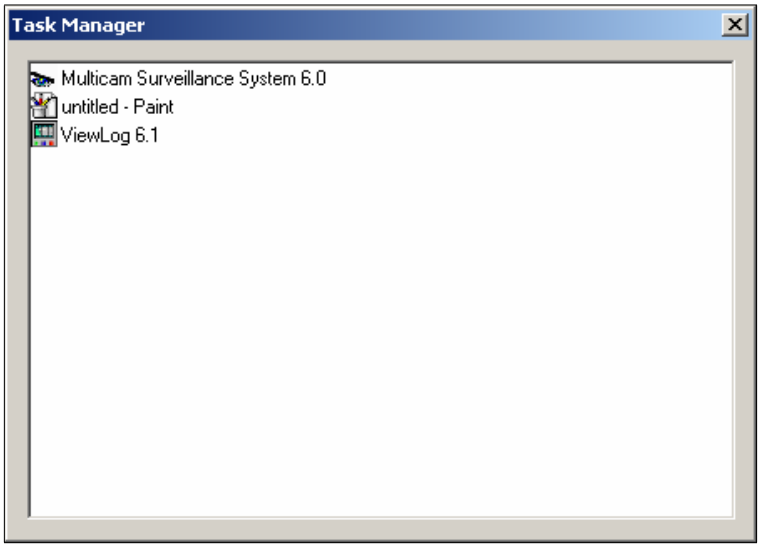


Figure 11-13

11.4.3 Token File for Save Mode

This option in the Settings section lets you export a token file. In case you enter safe mode and are in the status of the -Desktop, this token file will let you exit from the -Desktop and enter the Windows desktop. To export a token file and apply it, follow the steps below.

1. Click the **Export Token** button (Figure 11-12) to display the following dialog box.

Enter Token Code
In "Safe Mode(Boot)",users must locate "Token File" and enter "Token Code" to exit from the Multicam-Desktop.
Token Code:
123
Enter the Code up to 32 characters,with the combination of alphabets(ignoring case) and digits.
OK
Cancel

Figure 11-14

2. Type a code in the Token Code field.
3. Click **OK**. The Save As dialog box appears.

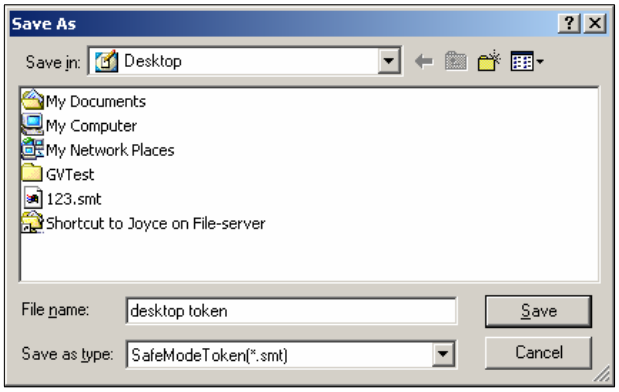


Figure 11-15

4. Locate a path, and enter a desired name in the File Name field.
5. Click **Save** to save the file.

   When you enter safe mode and are in the status of the -Desktop:
6. Click the **Settings** button on the desktop. You will be prompted to locate the stored token file and enter the set token code.
7. When the Settings window (Figure11-12) appears, select **Windows** in the Desktop Type field, and then exit from the window.
8. Click the **Log Off** button to log off the -Desktop and enter the Windows desktop. The token code and file are also required here.

11.5 Authentication Server

The Authentication Server is a password and account management system for multiple -Systems. The Authentication Server administrator can create the accounts with different access rights to a group of -Systems. Once the -System is connected to the Authentication Server, the previous password settings in local -Systems will be invalid. Local -Systems will submit to the full control of the Authentication Server.

11.5.1 Installing the Server

To install this application in a remote server, follow these steps:

1. Insert the Software DVD. It runs automatically, and a window appears.
2. Click **Install Sting Alarm Supplemental Utilities**.
3. Click **-Authentication Server**, and follow the on-screen instructions.

11.5.2 The Server Window

Go to Windows **Start**, click **Programs**, click **AuthServer** and click **AuthServer**. This window appears.

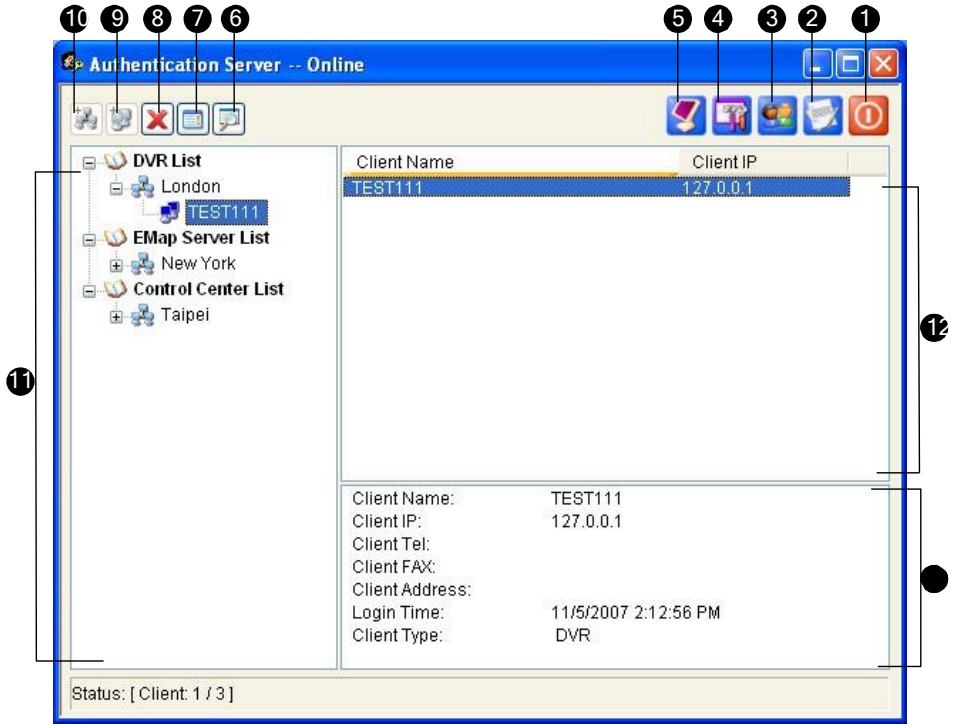


Figure 11-16

The controls in this window:

No.	Button	Description
1	Exit	Exits this window; Logs out Administrator; Changes Password, exports account information.
2	Log	Sets up the Authentication Server Log and opens the log browser.
3	Account Setup	Configures passwords and grants permissions to clients. Imports groups from Active Directory.
4	Server Setup	Configures the Authentication Server.
5	Start/Stop Service	Starts/Stops the Authentication Server.
6	Find A Client	Finds an existing client.
7	View/Edit A Client	Select a client from the Client List, and click to view /edit it.
8	Delete An Area /Client	Deletes an existing group or client.
9	Add A Client	Creates a client account.
10	Add An Area	Creates an Area group.
11	Client List	Lists the created clients and area groups.
12	Connected Client List	Lists the connected -Systems, E-Map Servers or Control Centers.
13	Client Information	Lists the information of the selected -System, E-Map Server or Control Center.

11.5.3 Creating a Client DVR

You must create and arrange client -Systems under the DVR List first. To create a DVR list, follow these steps:

1. To create a group, click the **Add An Area** button (No.10, Figure 11-16).
2. To create a client under the group, click the **Add A Client** button (No.9, Figure 11-16). This displays the Client Information dialog box.

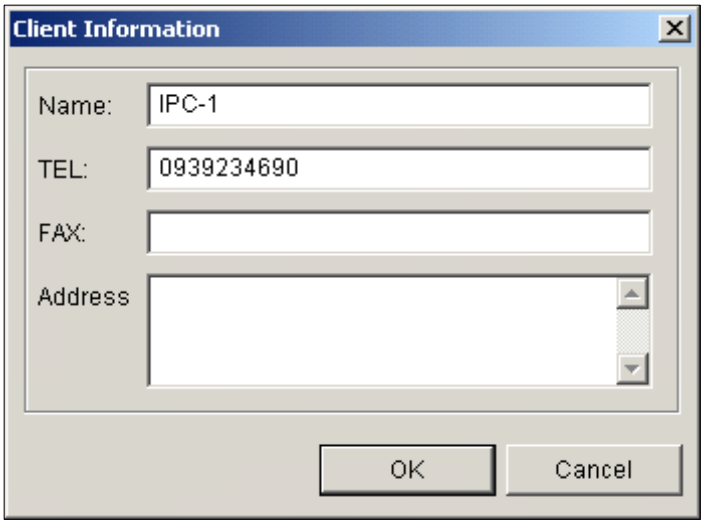


Figure 11-17 *Client Information*

3. Type the client's information. The Name must match that of local -System.
4. Click **OK**.

11.5.4 Creating a User Account

The Authentication Server administrator can create user accounts with different access rights to an assigned group of -Systems.

1. Click the **Account Setup** button (No.3, Figure 11-16) and select **Password Setup** to display the Password Setup window. The window is the same as the Password Setup window in Main System, except the following section.

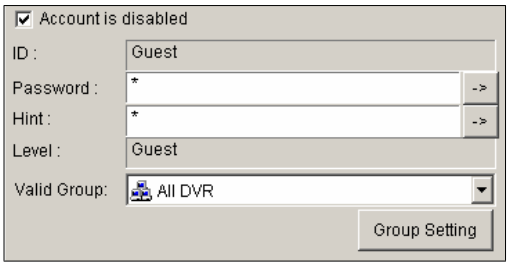


Figure 11-18 *Password Setup*

2. To create and edit a user account, refer to *Account and Password* in Chapter 1.
3. To grant the user access to a group of client -Systems:
   a. Click the **Group Setting** button in the window. The Valid Group List window appears.
   b. Click the **New Group** button. The DVR Group Information window appears.
   c. Name the DVR group, and select the desired -Systems into the group.
   d. Go back to the Password Setup window. Use the **Valid Group** drop-down list to select the created DVR group.

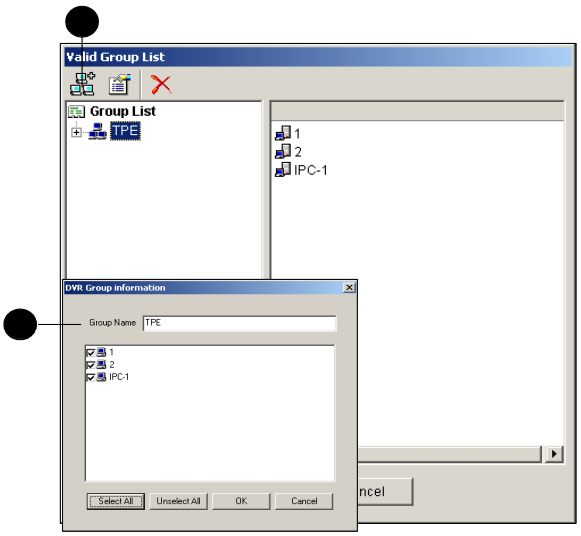


Figure 11-19

Note: In the Password Setup window of Authentication Server, the **Fast Backup & Restore** tab is not available.

11.5.5 Importing Groups and Users from Active Directory

To avoid creating user accounts manually, you can import groups and users from Microsoft's Active Directory to Authentication Server. You will need to install Active Directory on a Windows Server 2008 and set up users into groups the Active Directory before following the steps below.

Note:

1. This feature only supports Windows Server 2008.
2. User accounts in Active Directory need to be grouped into Groups settings first, because only groups can be imported into Authentication Server.

1. Click the **Account Setup** button (No.3, Figure 11-16) and select **AD Setup** to access the active directory setup page. This dialog box appears.

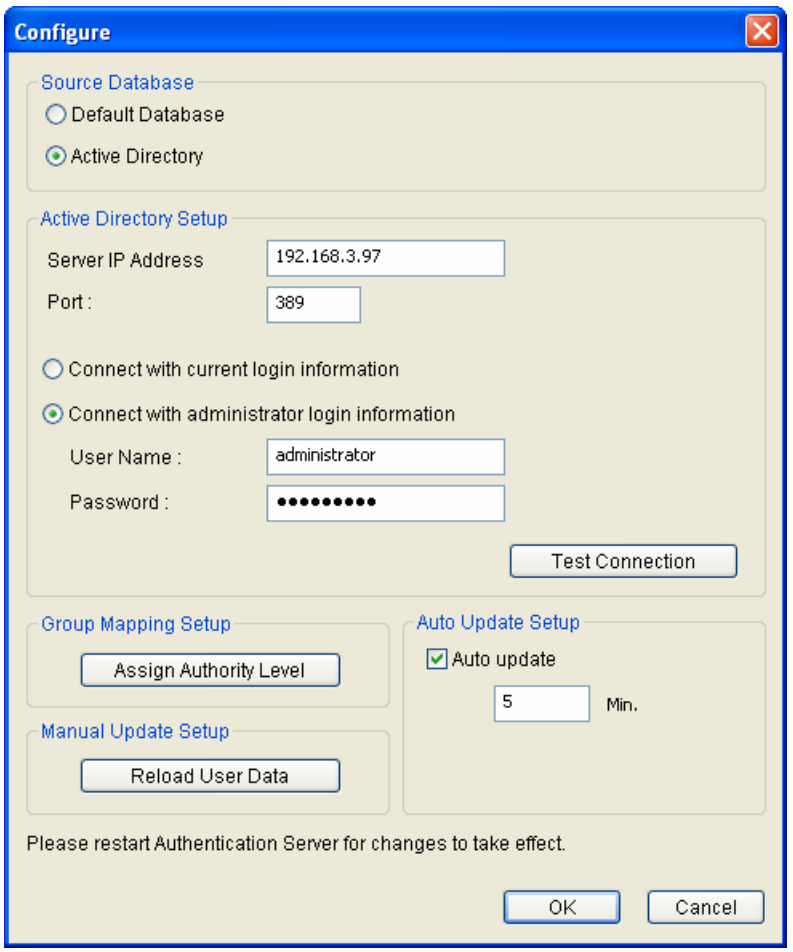


Figure 11-20

2. Under Source Database, select **Active Directory** to enable the function.
3. To connect to the server with Active Directory:
   a. Type the **Server IP Address** and the **Port** number of the server.

b. To log into the server using your current login information, select **Connect with the current login information**. To log into the server using the login information of its administrator, select **Connect with administrator login information** and type the User Name and Password.

c. Click **Test Connection** to see if you can connect to the server with Active Directory.

4. To assign groups in Active Directory to User, Poweruser or Supervisor authority levels:

a. Click the **Assign Authority Level** button. This dialog box appears.

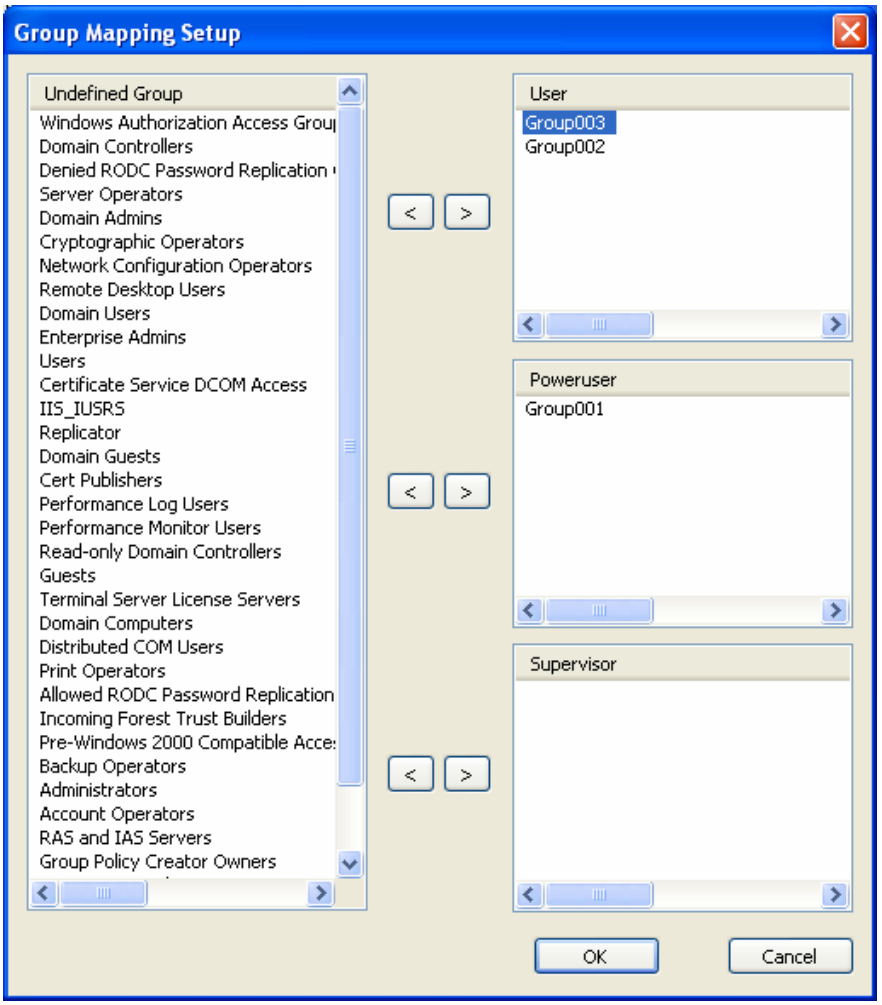


Figure 11-21

b. Select the groups detected in Active Directory from the left side and use the arrow buttons < > to assign the groups to User, Poweruser or Supervisor level.

c. Click **OK**. The user data will be imported into the Password Setup window.

5. To automatically update changes to user data in Active Directory, select **Auto Update** and type the update frequency in minutes.

6. To manually reload user data, click the **Reload User Data** button. Note that the current user data will be removed.

7. Click **OK** and restart Authentication Server to apply the settings.

11.5.6 Starting the Server

To configure the server and start the service, follow these steps:

1. Click the **Server Setup** button (No. 4, Figure 11-16). This dialog box appears.

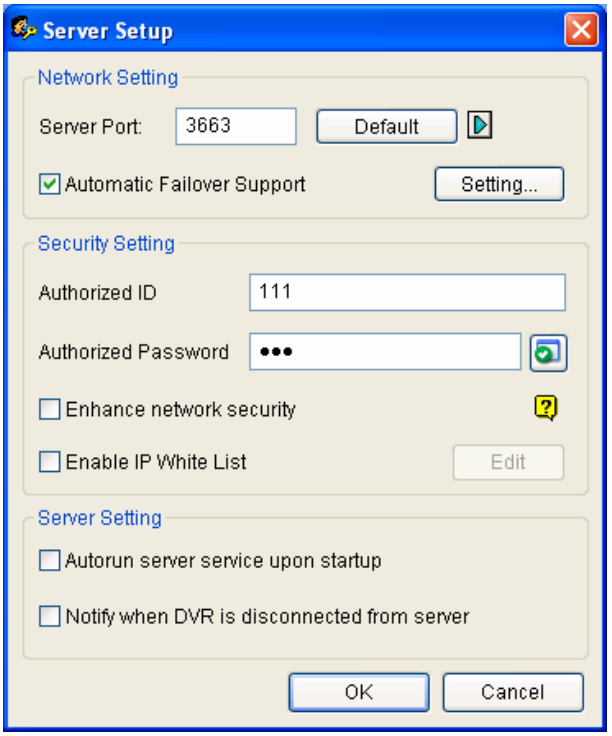


Figure 11-22 *Sever Setup*

2. Under Security Setting, type the **Authorized ID** and **Authorized Password** which will be used for the client -System to log into the Authentication Server.
3. Click **OK** to apply the settings.
4. Click the **Start/Stop Service** button (No. 5, Figure 11-16) to start the services.

You can optionally configure the following settings before starting the Authentication Server:

[Network Setting]

④ **Server Port:** The default port number is 3663. To use UPnP for automatic port configuration to your router, click the **Arrow** button. For details, see *UPnP Settings* in Chapter 8.

④ **Automatic Failover Support:** You can configure another two Authentication Servers in case of the primary Authentication Server failure. Once the primary server fails, the second or the third server will take over the connection from clients and provide uninterrupted services. Note the settings of Authorized ID and Authorized Password on the failover server must match those of the primary server. To set up the failover server, you can use the **Export Account** function in the **Exit** button.

Note: Once the primary Authentication Server is ready to resume the services, it is required to close the failover Authentication Server so the connection from clients can move back to the primary.

[Security Setting]

④ **Enhance network security:** Enhances network security on Authentication Server. Note after you enable the option, the client -System of version 7 or earlier cannot connect to the Authentication Server.

④ **Enable IP White List:** Click **Edit** to create a list of IP addresses allowed to connect to Authentication Server.

[Server Setting]

④ **Auto start service upon server startup:** Starts automatically the service when Windows starts.

④ **Notify when DVR disconnected from server:** Notifies the Authentication Server with a pop-up window when the -System and Authentication Server loss connection.

11.5.7 Connecting -System to the Server

To configure the -System in order to access the Authentication Server remotely through a network connection, follow these steps:

1. Click the **Configure** button (No. 14, Figure 1-2), point to **System Configure**, select **Password Setup**, and then select **Remote Authentication Setup**. This dialog box appears.

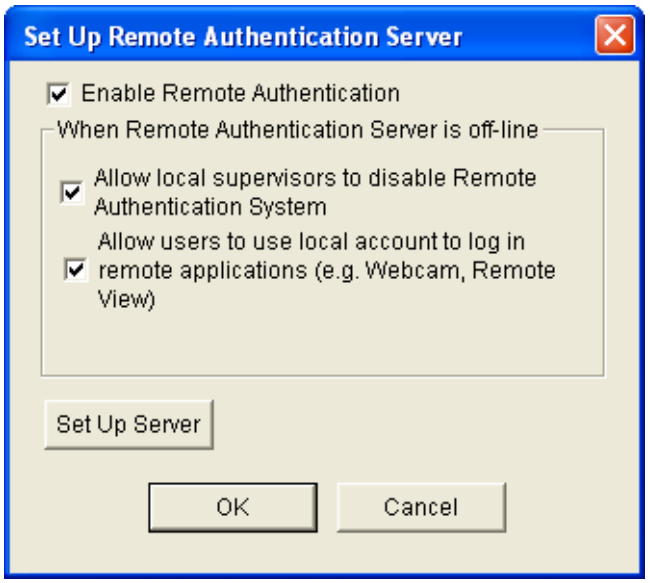

Set Up Remote Authentication Server
Enable Remote Authentication
When Remote Authentication Server is off-line
Allow local supervisors to disable Remote Authentication System
Allow users to use local account to log in remote applications (e.g. Webcam, Remote View)
Set Up Server
OK
Cancel

Figure 11-23

④ **Enable Remote Authentication:** Enable the connection with the Authentication Server.

④ **Allow local supervisors to disable Remote Authentication System:** Allows the local supervisor to stop the Authentication application when the connection with the Authentication Server fails. Note if the option is disabled and the connection with the Authentication Server fails, the local supervisor will not be able to log into the -System and the dialog box won't be accessible until connection resumes.

④ **Allow users to use local account to log in remote applications:** Allows the local users to access other remote applications with their previous password and ID settings when the connection with the Authentication Server fails.

2. Click the **Set Up Server** button in Figure 11-23. This dialog box appears.

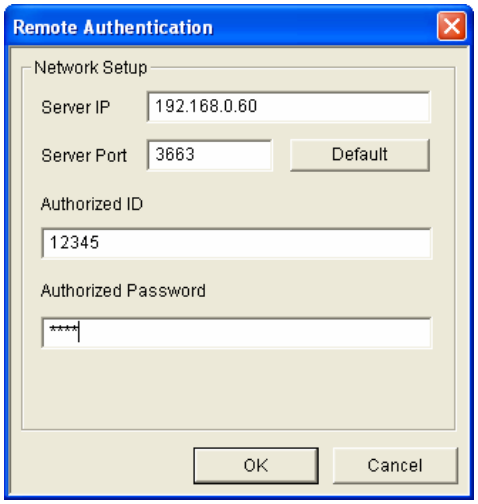


Figure 11-24

3. Enter the IP address and port of the Authentication Server. Type the **Authorized ID** and **Authorized Password** of the Authentication Server (Figure 11-24).
4. Click **OK** to start the connection. **When the connection is established, the previous password settings in the -System will be invalid.**
5. Press **[L]** on the keyboard to call up the Login dialog box. The icon indicates the connection is established.

Figure 11-25

As long as the Authentication Sever is working, every time when you start the -System, the Login dialog box will appear. Enter the user account created on the Authentication Server to log into the server.

Note: When the disconnection icon appears on the Login dialog box (Figure 11-25), there might be one of these three reasons:

1. The login ID and Password do not match any of user IDs and Passwords created on the Authentication Server.
2. The client's given name (Figure 11-17) doesn't match the -System's.
3. The network connection has traffic problem.

11.5.8 Remote Access from Control Center, Remote E-Map and MultiView

The Authentication Server allows you to restrict users of E-Map Server, Control Center, and MultiView to access specific DVR hosts and cameras only. Instead of connecting to DVR hosts directly, the user of E-Map Server, Control Center and MultiView will connect to the Authentication Server using the user account you created on the Authentication Server.

You must first set up remote authentication on E-Map Server and Control Center. After E-Map Server, Control Center and MultiView are connected to the Authentication Server, the user will be prompted to log in with the user ID and password you created on the Authentication Server. Once logged in, a list of DVR hosts authorized to the user account will be displayed, and the user will be able to view the assigned cameras.

Setting Authentication Server

You need to create and arrange E-Map Servers and Control Servers under their separate lists on the Authentication Server window (Figure 11-16). Type the name and information of the E-Map Server or Control Center in the Client Information dialog box. The name does not need to match the location name of the E-Map Server or Control Center.

Accessing from E-Map Server

The E-Map Server can access the user account setting of the Authentication Server.

1. In the E-Map Server window, click **Tools** on the menu bar, and select **Options**. This dialog box appears.

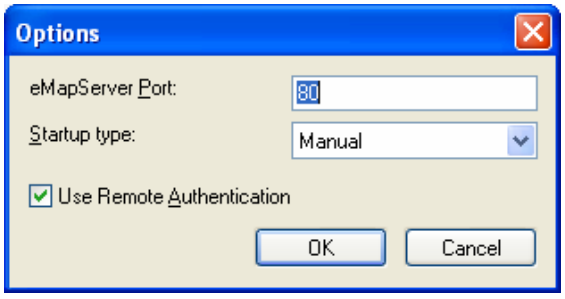


Figure 11-26

2. Select **Use Remote Authentication**. If you want the Authentication Server service started automatically at Windows startup, select **Automatic**. Keep the Port 80 as default or change it if necessary. Click **OK**.

3. Click **Tools** on the menu bar, and select **Remote Authentication**. This dialog box appears.

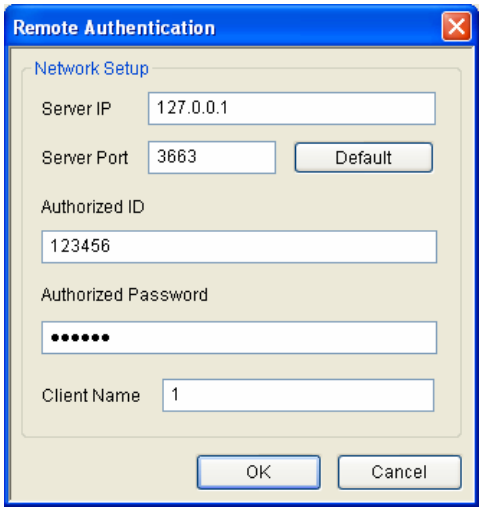


Figure 11-27

4. Type the IP address, authorized ID and authorized password of the Authentication Server. Type the E-Map Server's client name created on the Authentication Server. Click **OK**.
5. Click the **Start Service** button on the toolbar to start the E-Map Server.
6. When you log into the E-Map Server, enter the user ID and password created on the Authentication Server. A list of assigned -System hosts to the user will be displayed.

Accessing from Control Center

The Control Center can access account settings of the Authentication Server.

1. On the Host List, right-click **Host List by ID** and select **Remote Authentication Setup**. A dialog box appears. See Figure 11-27.
2. Type the IP address, authorized ID and authorized password of the Authentication Server. Type the Control Center's client name created on the Authentication Server. Click **OK** to enable connecting to the Authentication Server.
3. To access the Authentication Server account settings, on the Host List, right-click **Host List by ID** and select **Get Host List by ID**. A dialog box prompts you for ID and password.
4. Type a user ID and password created on the Authentication Server, and click **OK**. A list of assigned -System hosts to the user will be displayed.

Accessing from Multi View Viewer

Once the -System is connected to the Authentication Server, you can only enter the user account created on the Authentication Server to log into the Multi View Viewer. Once you log into the Multi View successfully, a list of assigned -System hosts to the user will be displayed.

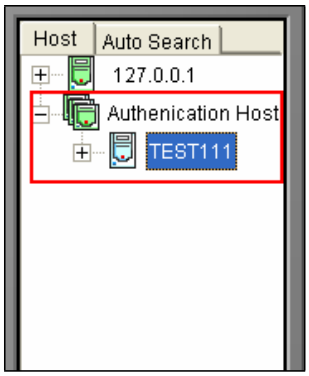


Figure 11-28

11.6 Fast Backup and Restore

With the Fast Backup and Restore (FBR) solution, you can change interface skin and customize features to suit personal preference, as well as back up and restore your configurations in Main System.

11.6.1 Installing the FBR Program

1. Insert the Software DVD, click **Install Sting Alarm Supplemetal Utilities**, select **-Fast Backup & Restore Multicam System**, and follow the on-screen instructions.
2. After the installation is complete, run **Fast Backup & Restore Multicam System** from the Windows Start menu. This window appears.

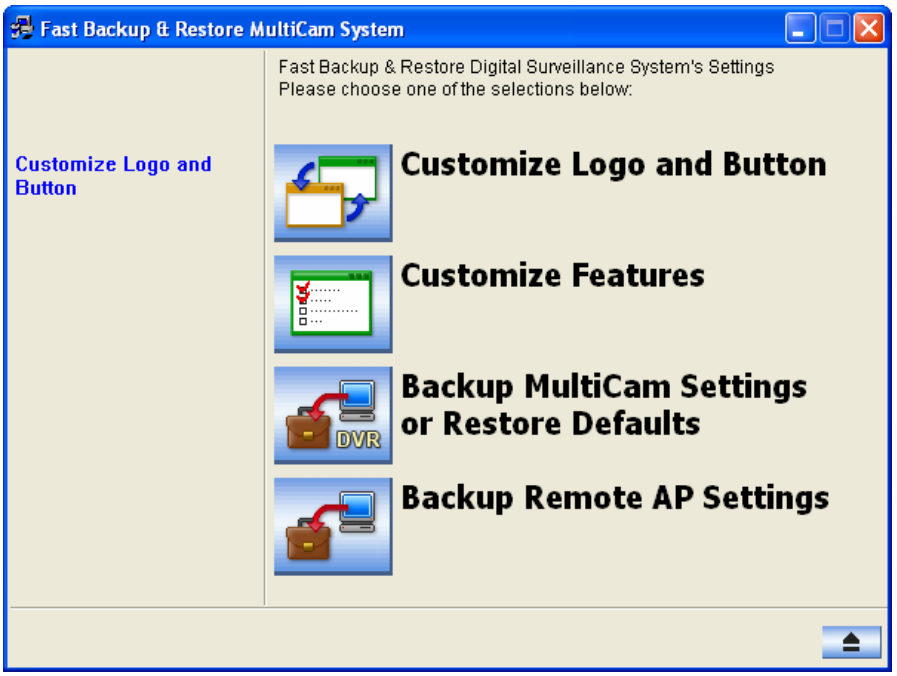

Fast Backup & Restore MultiCam System
Fast Backup & Restore Digital Surveillance System's Settings
Please choose one of the selections below:
Customize Logo and Button
Customize Logo and Button
Customize Features
Backup MultiCam Settings or Restore Defaults
DVR
Backup Remote AP Settings

Figure 11-29

11.6.2 Customizing Logo and Button

You can replace the screen images of Startup Splash, Non-Active Video and Video Lost with your own images.

Before you start, remember that each screen image has its specified size. Create your own image according to these specifications:

- **Startup Splash:** Bit Depth 24, Width 316, and Height 272.
- **Non-Active Video:** Bit Depth 24, Width 720, and Height 576.
- **Video Lost:** Bit Depth 24, Width 720, and Height 576.

To customize the screen image, follow these steps:

1. In the FBR window (Figure 11-29), click the **Customize Logo and Button** icon, select **DVR**, and then select **Custom Logo**. This window appears.

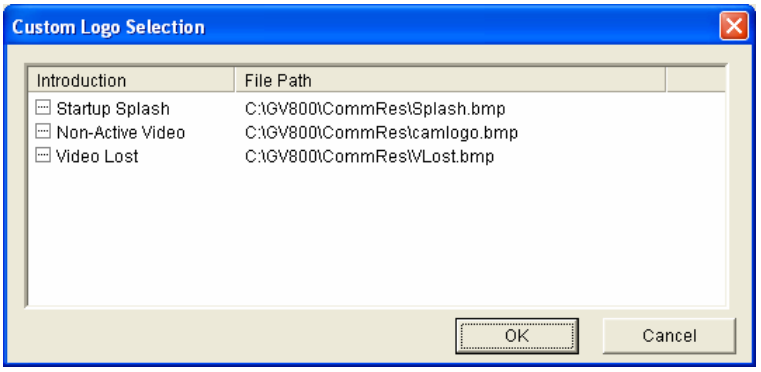


Figure 11-30

2. Click a desired screen image to be replaced with an imported image.
3. Exit the FBR program, and start the -System to see the change.

11.6.3 Customizing the Features

Not every feature may be of equal interest to you. You can now specify which features are to be displayed at system startup.

1. In the FBR Window (Figure 11-29), click the **Customize Features** icon to display this dialog box.

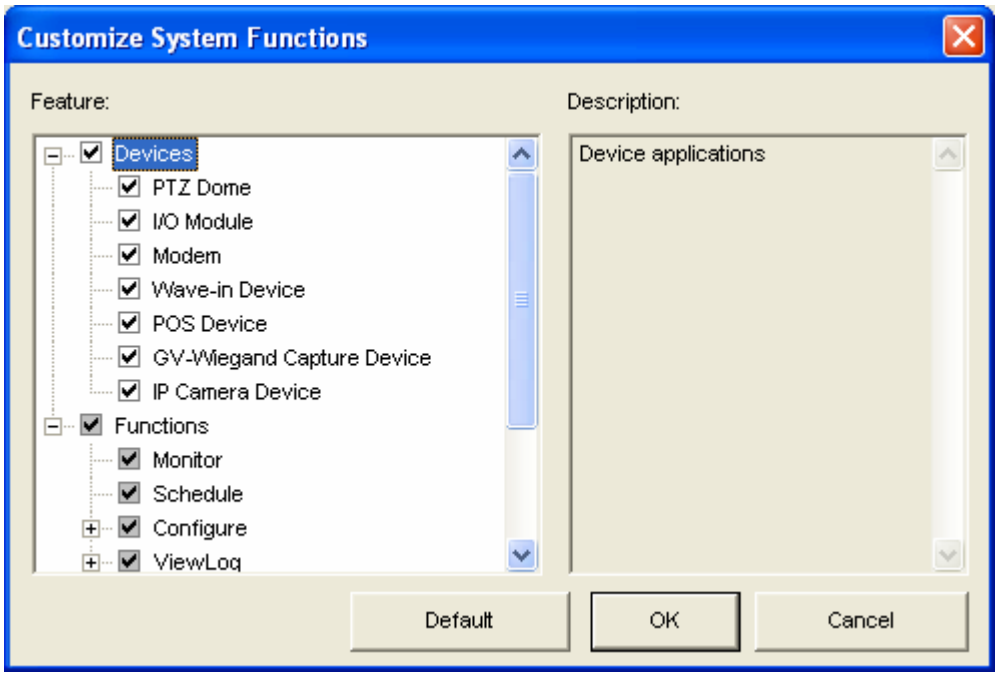


Figure 11-31

[Devices] Expand this folder, and select the device applications you want to enable in the -System.

[Functions] Expand this folder, and select the functions you want to enable in the -System. The gray checked boxes indicate that the functions are enabled by default. No changes can be made to these functions.

2. Click **OK** to apply the settings.

11.6.4 Backing up and Restoring Settings

You can back up the configurations you made in Main System, and restore the backup data to the current system or import it to another -System.

Backing up the settings

1. In the FBR window (Figure 11-29), click the **Backup System Settings or Restore Defaults** icon, and select **Backup Current System**. This dialog box appears.

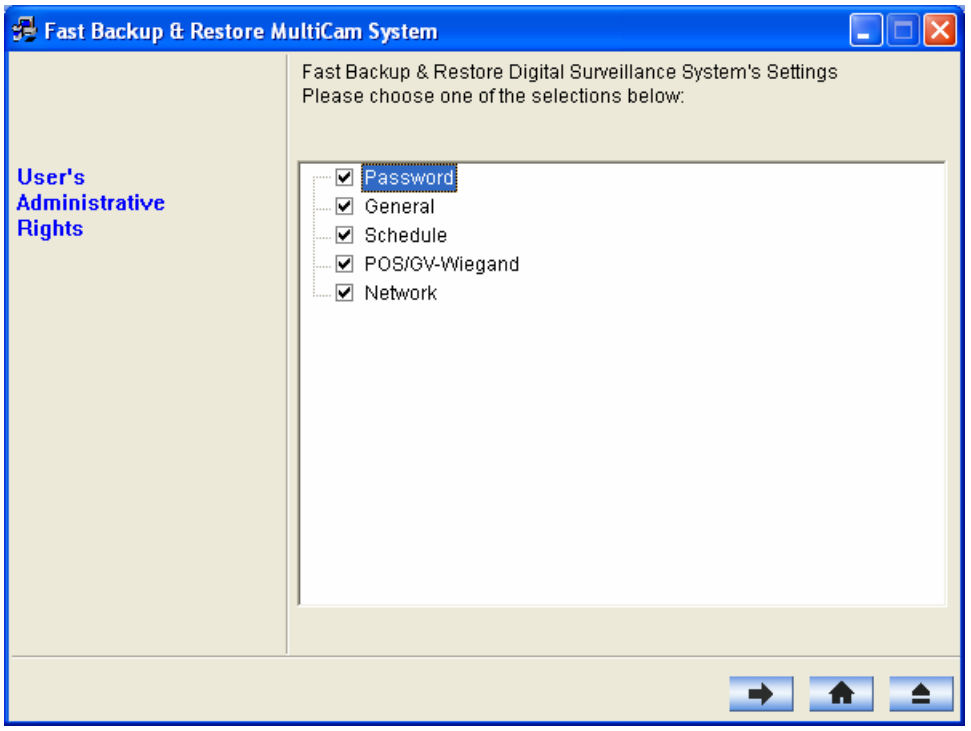


Figure 11-32

2. Select which settings you want to back up, and press the **Next Step** button . The Save As dialog box appears.
3. Select the destination drive to store the backup file. When the backup is complete, this message will appear: *Successfully Backup MultiCam System Settings*.

Restoring the System

You can restore the current system with the backup of configuration file. Also, you can copy this backup file to configure another system with the same settings as the current system.

1. Open the backup file (*.exe) you previously stored. A valid ID and password are required to display this window.

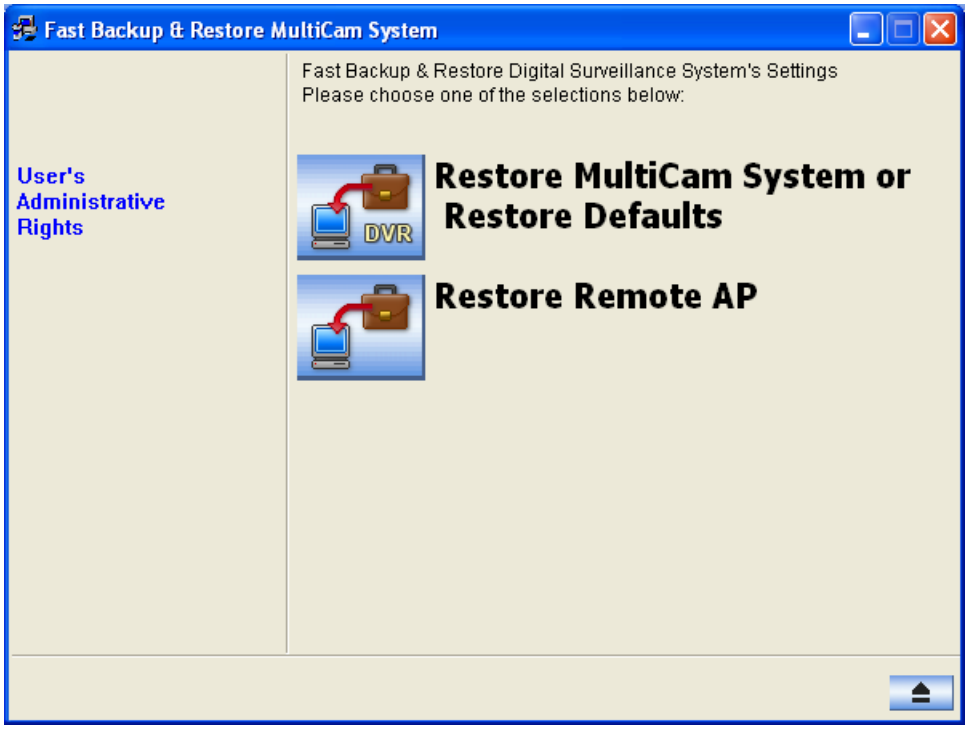

Fast Backup & Restore MultiCam System
Fast Backup & Restore Digital Surveillance System's Settings
Please choose one of the selections below:
User's Administrative Rights
DVR
Restore MultiCam System or Restore Defaults
Restore Remote AP

Figure 11-33

2. Click the **Restore Multicam System** icon, and then select which backup settings you want to restore.
3. Press the **Next Step** button to start restoring.
4. When the restoration is complete, this message will appear: *Successfully Restore MultiCam System Settings*.

Restoring Defaults

You can choose to restore the system default settings by clicking the **Backup System Settings or Restore Defaults** icon, and select **Restore Defaults**.

Note: Files backed up from -System V8.5.6.0 or before can be imported or restored back to -Systems using Windows 8 or Server 2012 by disabling the User Account Control (UAC) for the operating systems. Windows 8 and Server 2012 are only supported in -System V8.5.7.0 or later.

11.7 Hot-Swap Recording

The program Media Man Tool provides a hot-swap feature, allowing a non-stop recording. You can add and remove a hot-swap or portable hard drive to the -System without interrupting the monitoring. When the new drive is added, it will be configured to the recording path automatically.

Additionally, you can back up ViewLog player and database files to play back at any computer.

Note: The hot-swap feature supports the disk capacity of 2 GB at least.

11.7.1 The Media Man Tool Window

This program comes with the installation of Main System. Click Windows **Start**, point to **Programs**, select the folder and then select **Hot Swap HDD Tool.** This window will appear.

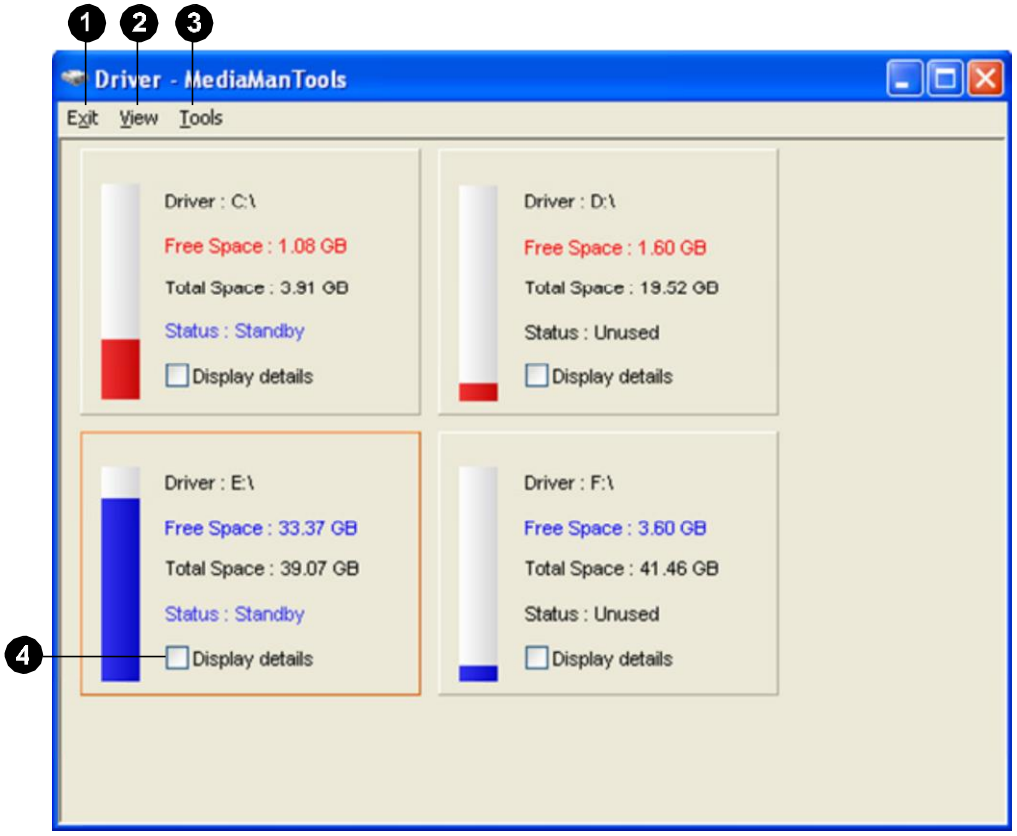


Figure 11-34

The controls in this window:

No.	Name	Description
1	Exit	Closes or minimizes the Median Man Tool window.
2	View	Refreshes the disk drive status shown in this window.
3	Tools	Sets up the LED panel and automatically logs in the Media Man Tool window.
4	Display Details	Select the option to view the status and information of the disk drives. For details, see *Viewing Disk Drive Status* later in this chapter.

11.7.2 Viewing Disk Drive Status

To view the detailed information of a drive, check **Display Details** (No. 4, Figure 11-34) in the desired drive section. The status window will appear.

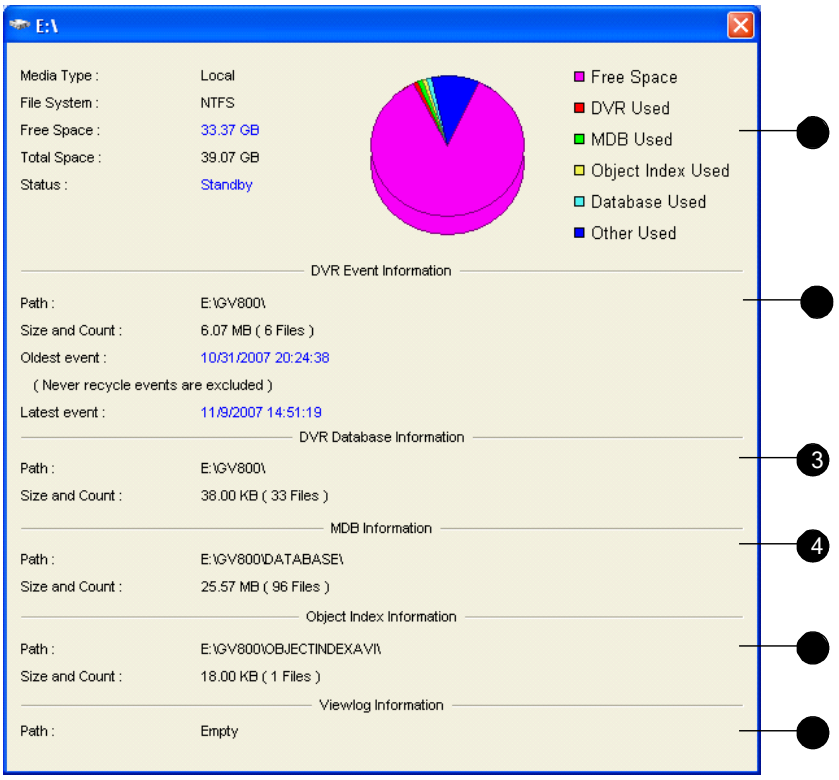


Figure 11-35

The controls on the MediaMan window:

No.	Name	Description
1	Disk Properties	Indicates disk information. In “Media Type,” two messages may appear: ⌘ **LAN:** indicates a hard drive is connected. ⌘ **Local:** indicates a local hard drive is connected. In “Status”, three messages may appear: ⌘ **Standby:** indicates the hard drive already specified as the recording path. ⌘ **Unused:** indicates the hard drive not specified as the recording path. ⌘ **Recording:** indicates the files are being recorded to the disk.
2	DVR Event Info	Indicates the path, size and number of recorded events; the dates of the oldest and latest events.

3	DVR Database Info	Indicates the path, size and number of the ViewLog Event List log files.
4	MDB Info	Indicates the path, size and number of System Log files.
5	Object Index Info	Indicates the path, size and number of Object Index files.
6	ViewLog Info	Indicates the location you have backed up the EZ ViewLog player.

Note: The DVR Event Info updates every minute. The MDB Info, DVR Database Info, Object Index Info and ViewLog Info update as data changes.

11.7.3 Adding a Disk Drive

1. Click Windows **Start**, point to **Programs**, select the folder and select **Hot Swap HDD Tool**.
2. Insert a hot-swap hard drive or plug a portable hard drive to your computer. This dialog box appears.

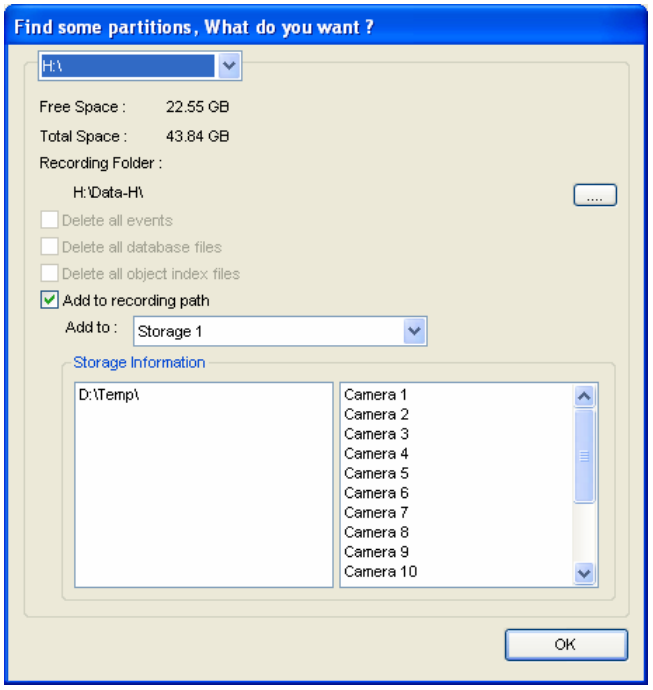


Figure 11-36

3. Select **Add to recording path** and select the storage group from the drop-down list.
4. If there are recording files saved on the hard drive, you may select the options of **Delete all events**, **Delete all database files** or **Delete all object index files**.
5. Click **OK** to automatically configure the hard drive to the recording path.
6. To verify the hard drive is added successfully, check if the "Status" of the drive displays *Standby*. Or in the Main System, click the **Configure** button, point to **System Configure**, select **General Setting**, click the **Set Location** button, and then select the **Storage Group Folder** to confirm the new recording path.

Tip: To add a local drive to the recording path, right-click the desired drive, select **Add for recording** and follow Step 3 to add the drive.

11.7.4 Removing a Disk Drive

To remove a disk drive from the recording path, right-click the desired drive, and select **Remove from recording path**. This dialog box will appear. You can export related database files with the recordings on the hard drive. You can also export the ViewLog player which allows you to play back the recordings on any computer.

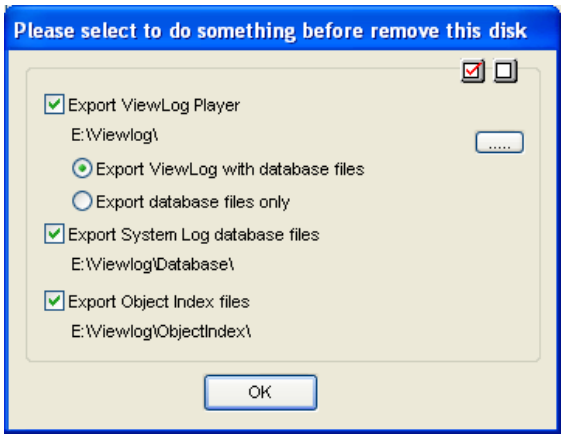


Figure 11-37

④ **Export ViewLog Player:**

- **Export ViewLog with database files:** Exports the ViewLog player together with ViewLog Event List log files (.db files), related to the recordings on the hard drive.
- **Export database files only:** Exports ViewLog Event List log files (.db files) only if the ViewLog program already exits on the hard drive.

④ **Export System Log database files:** Exports the system log files (.mdb files), related to the recordings on the hard drive.

④ **Export Object Index files:** Exports the Object Index files, related to the recordings on the drive.

④ **[…] button:** If you want to change the default folder “Viewlog” created on the hard drive, click the button.

Note: Removing the hard drive will affect ViewLog database. To restore these events, add the hard drive back to the system and run **Repair Database Utility**.

11.7.5 Logging In Automatically at Startup

To automatically log in and minimize the Media Man Tools window at Windows startup, follow these steps:

1. Click **Tools** on the menu bar, and select **Auto login at Windows startup**. A dialog box appears.
2. Type the ID and password of the -System for automatic login in the future.
3. If you want to minimize the Media Man Tools window to the system tray at startup, select **Auto minimize at startup**.
4. Click **OK** to apply the settings.

11.7.6 Setting LED Panel

A LED panel on the screen provides a quick indication of the activity status of hard disk drives.

Figure 11-38

LED Color	Description
Gray	No HDD is assigned to this LED.
Green	A HDD is assigned to this LED.
Red	The HDD is full.
Flashing Green	-System is recording or the video / audio files are played back in ViewLog.
Flashing Red	The HDD is recycling.

1. Click **Tools** on the menu bar and select **Setup LED Panel**. This dialog box appears.

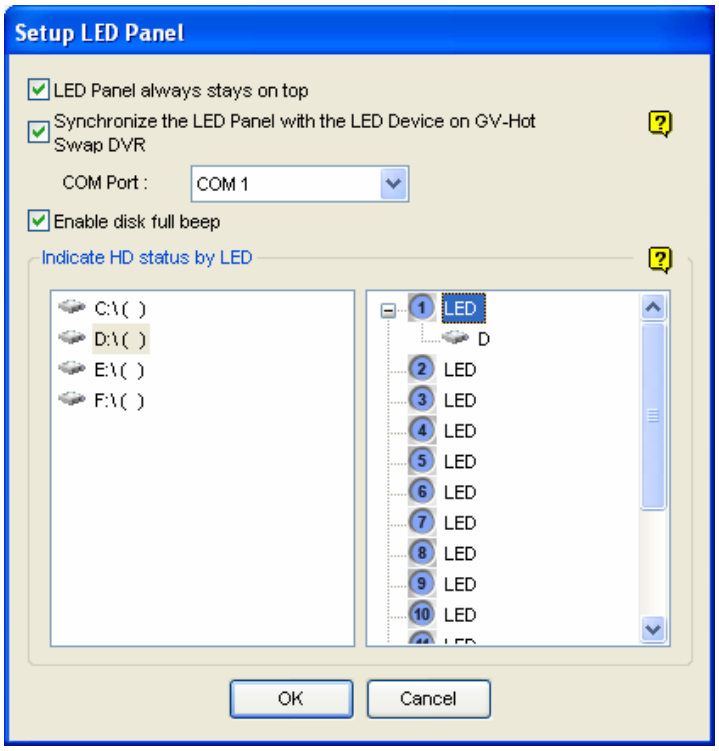


Figure 11-39

④ **LED Panel always stays on top:** This option makes the LED panel stay on top of other windows when the Media Man Tools window is minimized.

④ **Synchronize the LED Panel with the LED Device on -Hot Swap DVR:** This option is designed for the use of the -Hot Swap DVR System. When this option is enabled, the LED device installed on the front panel of the -Hot Swap DVR System will synchronize with the LED panel on the screen.

④ **Enable disk full beep:** When the hard disk drive is full, the system sounds on. Note this function only works when the motherboard is equipped or installed with a PC speaker.

2. By default, only the hard disk drive that stores video and audio files will be assigned to LED. If you want to re-assign the hard disk drive or assign other drives to LEDs, freely move the hard disk drive to the desired LED on the tree.
3. Click **OK** to apply the settings, and minimize the Media Man Tool window to display the LED panel on the screen.
4. If you want to return to the Media Man Tools window, right-click the LED panel and select **Switch to the setup window**.

Note:

1. Because the LEDs are designed to indicate the video and audio files are being written or read, it is not recommended to assign the HDDs that store log files to the LEDs.
2. If the HDD that stores log files is assigned to a LED and its LED turns red, make sure the log files are not being written before you remove it. Otherwise, the log files might be lost during the removal. For details on storage locations of logs and video/audio files, see *Setting Data Storage* in Chapter 1.

11.8 Backup Server

With Backup Server, the -System can back up recorded files to the storage system over Internet. When the Backup Server is enabled, a copy of recorded files will automatically be backed up to the storage system.

The Backup Server can support any storage system protocol which can add itself to Windows and be formatted by Windows Disk Management. The following diagram shows the possible types of storage systems the Backup Server can support. The Backup Server allows you to select multiple drives, both local drives or through networking, to be used to back up files.

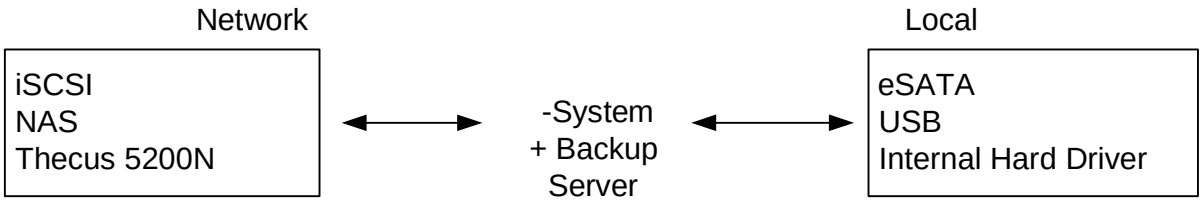


Figure 11-40

11.8.1 Adding a Disk Volume

Generally the steps to add a disk volume from a storage system looks something like this:

1. Assign a disk volume on the storage system for -System.
2. Create an account on the storage system for -System.
3. Build the connection between the storage system and -System. Certain storage systems may require you to install and configure additional program, e.g. iSCSI Initiator, on the computer of -System for building the connection. For this, consult the documentation of your storage system.
4. When the disk volume can be detected by Windows, format the disk volume with Window's Disk Management as well as a lock disk.

Steps 1~3 may vary depending on the type of storage system. Ensure the newly added storage drive can be detected by Windows and be formatted by **Disk Management** in Computer Management. (To access the Computer Management window, right-click the **My Compute**r icon on the desk and select **Manage**. Go down to **Storage** and select **Disk Management**.)

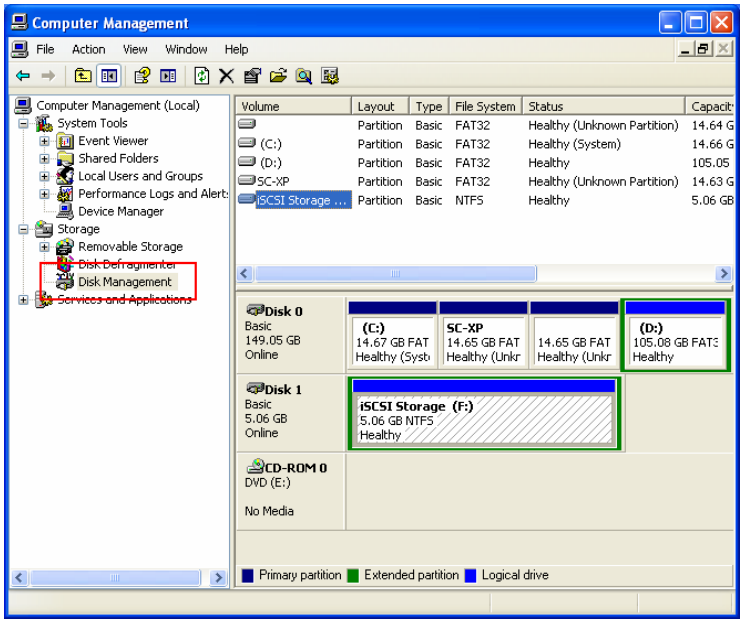


Figure 11-41

Note:

1. It is recommended that the formatted partition should be **Basic disk storage** and **NTFS file system** if the disk volume is over 32 GB.
2. For users of the iSCSI storage system, a node name account should only be applied for one host/computer to use. It is restricted to apply one node name account on different hosts/computers due to data conflict.

11.8.2 Enabling Backup Server

Before you activate the Backup Server, ensure the connection between the storage system and -System has been built and newly-added disk volumes have been formatted as well.

1. On the -System, click the **Network** button (No. 11, Figure 1-2), and select **Backup Server**. The Geo Backup Server dialog box appears.
2. Click the **Edit** button and select locations to store the backup files.
3. Select **Copy Viewlog to backup drives** if you want to copy the ViewLog application to each of the partition selected.
4. Click **OK**.
5. Click the **Login** button to connect to the storage system.

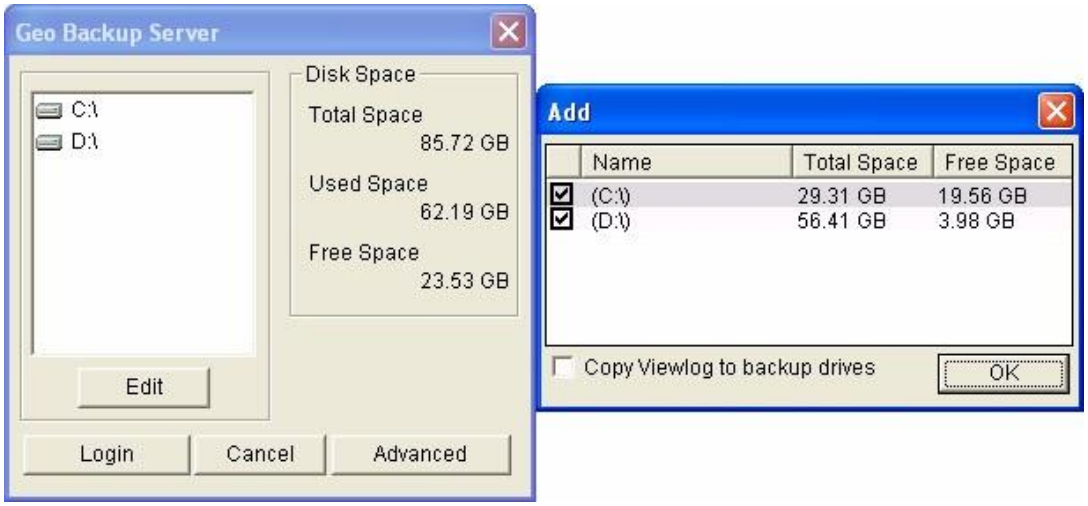


Figure 11-42

Note: When **Copy Viewlog to backup drives** is selected, a **ViewLog** folder and **Backup Server Viewlog.bat** will be created in the selected partitions after backup is completed. Double-click **Backup Server Viewlog.bat** to run ViewLog and to load the recorded events into ViewLog.

11.8.3 Advanced Settings

You may want to configure the Backup Server to fit into your own needs. In the Geo Backup Server dialog box (Figure 11-42), click **Advanced**. The Advanced Settings dialog box appears.

[General]

You can select the bandwidth speed to ensure the quality connection.

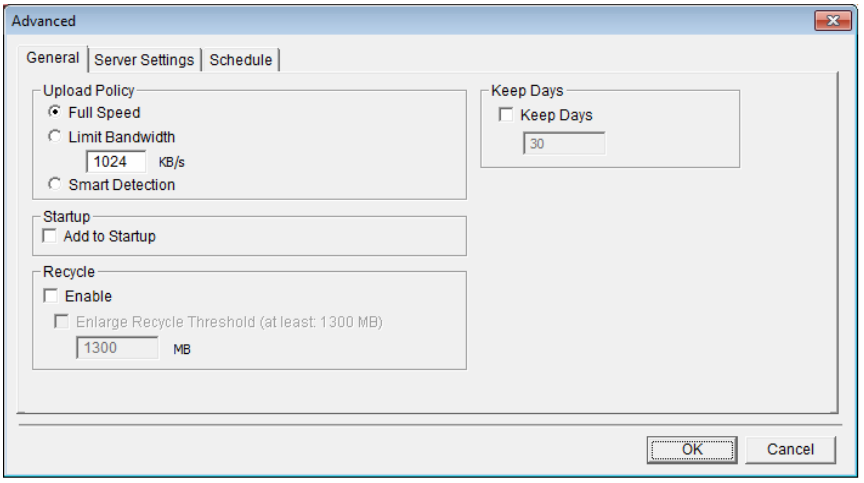


Figure 11-43

[Upload Policy]

④ **Full Speed:** Build the connection at full maximum speed.

④ **Limit Bandwidth:** Specify the desired bandwidth limit in kb/s.

④ **Smart Detect:** Automatically detect the file size and decide the proper bandwidth speed.

[Startup] Automatically starts the Backup Server at Windows startup.

[Recycle] Enable this option to recycle video files.

④ **Enlarge Recycle Threshold:** Recycle threshold is the file size at which the recycling begins. If you set the recycle threshold to be 2000 MB, recycling starts when free space on the connected disk is under 2000 MB and the oldest files are overwritten. The upper limit of the recycle threshold is 99999 MB.

[Keep Days (1-999)] Specify the number of days to keep the files from 1 day to 999 days. When both **Keep Days** and **Recycle** are enabled, the system applies whichever condition comes first. For example, if the specified smallest amount of storage space comes earlier than the designated keep days, then recycle is applied first.

[Server Settings]

You can select the files of cameras to be backed up, and the notification method when the network is disconnected.

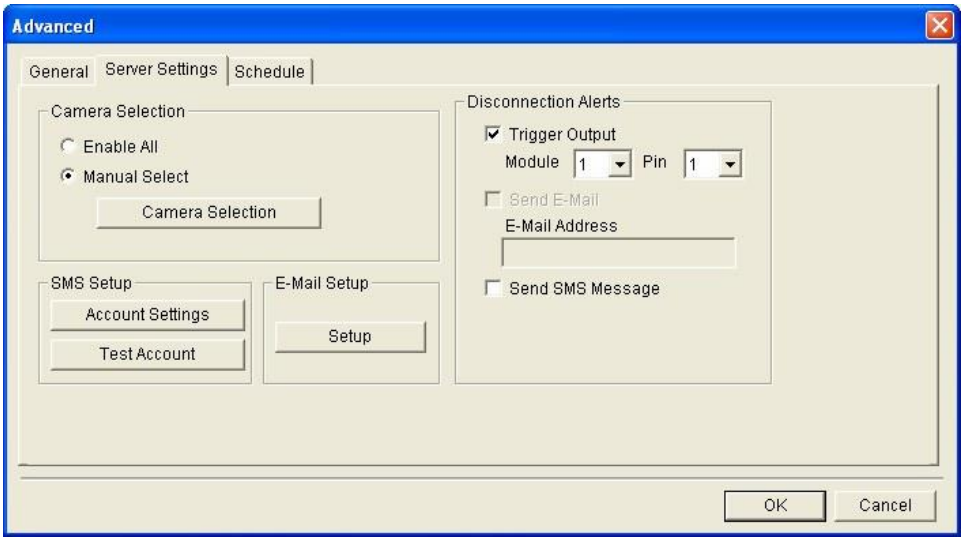


Figure 11-44

④ **Camera Selection:** Selects the files of desired cameras to be backed up.

④ **Disconnection Alerts:** Selects the alert methods when the network is disconnected.

- **Trigger output:** Triggers the specified output module and pin for alerts.
- **Send E-mail:** An e-mail message is sent out for alerts. Before using this function, click the **Setup** button in the E-Mail Setup field to set up an e-mail account.
- **Send SMS Message:** A SMS message is sent out for alerts. Before using this function, click the **Accounts Settings** button in the SMS Setup field to set up a SMS account.

[Schedule]

You can plan the time to back up the files to the storage system.

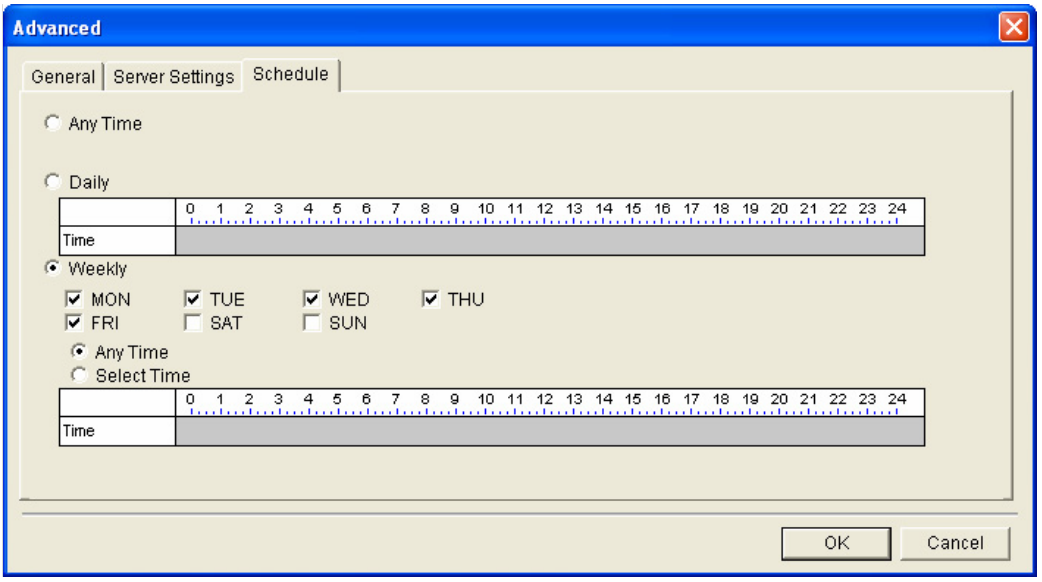


Figure 11-45

④ **Any Time:** The backup starts whenever there are files to be backed up.

④ **Daily:** The backup starts at the set time of a day. Drag the mouse over the timeline to define the start and end time.

④ **Weekly:** The backup can start at any time or the specified time of a week. To specify the time, select the desired days (Mon – Sun), select **Select Time**, and then drag the mouse over the timeline to define the start and end time.

11.8.4 Manually Adding Files for Backup

Once connected, the files from the -System will automatically be backed up to the storage system. To manually select the files for backup:

1. Click the **Backup Server** icon on the system tray, and then select **Add Files**. This dialog box appears.

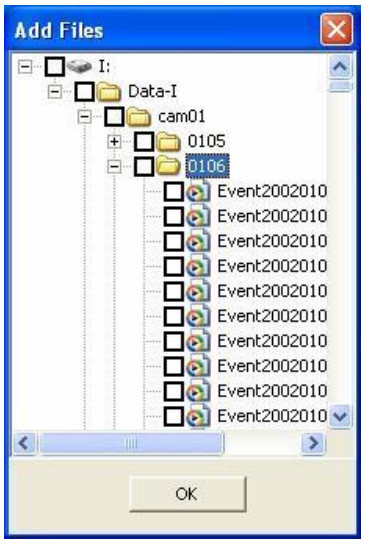


Figure 11-46

2. Expand the hard disk drive folders and select the files for backup.
3. Click **OK** to start.

11.8.5 Viewing Server Status

You can access the information of connection activities, backup files and backup data. To view the information, click the Backup Server icon on the system tray and select **Server Status**. The Upload Info dialog box appears.

[Event Log]

This tab shows the history of connection activities. Note that the latest event is always placed on the top.

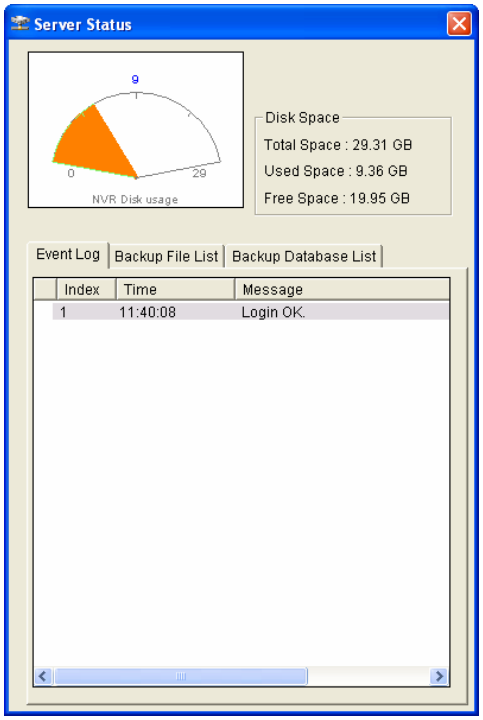


Figure 11-47

[Backup File List]

This tab displays the files being backed up. Click **File View** to display the backup files by file names or click **Camera View** to display the backup files by cameras.

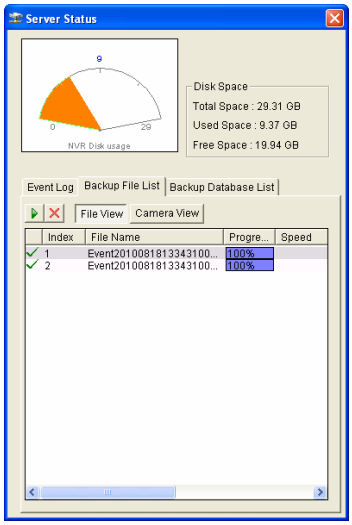


Figure 11-48

Tip: To view the information of the backup file, click the file event.

[Database List]

The related log data, including system log and POS data, will be backed up to storage system with the recording files. Note that the record only appears on the next day of file transference.

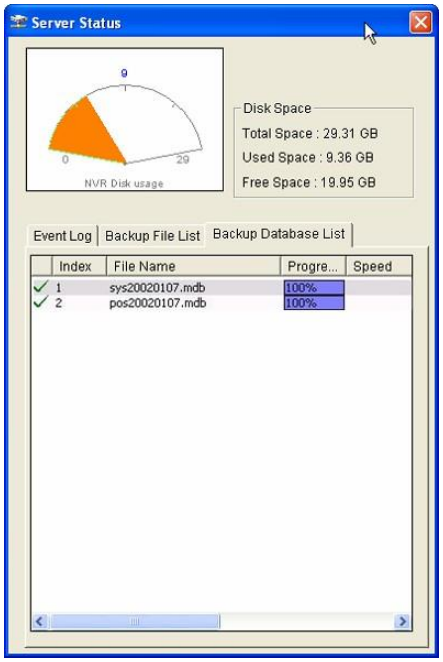


Figure 11-49

11.8.6 Retrieving Recorded Files

You can retrieve the files from the storage system and play video back.

1. On the ViewLog screen, click the **Tools** button (No. 6, Figure 4-2), and select **Remote Storage System**. This dialog box appears.

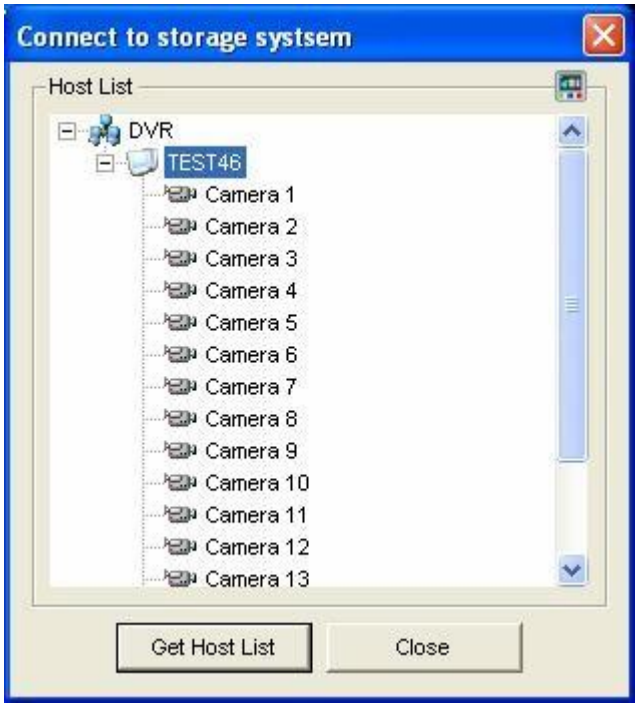


Figure 11-50

2. Click the **Get Host List** button to enable connecting to the storage system. The DVR icon appears.
3. Expand the DVR folder, select the host and click the button on the top right corner.
4. After the events stored on the storage system are displayed on the Event List, you can use ViewLog features for playback.

11.8.7 Viewing Backup Status

You can view the backup status of each camera. To view the information, click the Backup Server icon on the system tray and select **Backup Status**. The Backup File Viewer dialog box appears. In the left menu, click a camera channel to see the date and time when the recording of the camera was backed up.

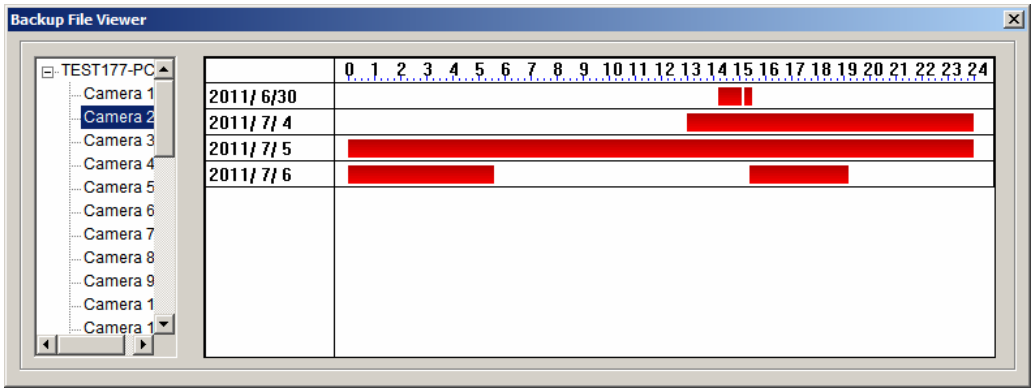


Figure 11-51

11.9 Backup Viewer

With the Backup Viewer, you can access the video recordings and log data backed up at the storage system from any computer over the Internet. You can search the log data as well as view, edit and save the recordings at the local computer.

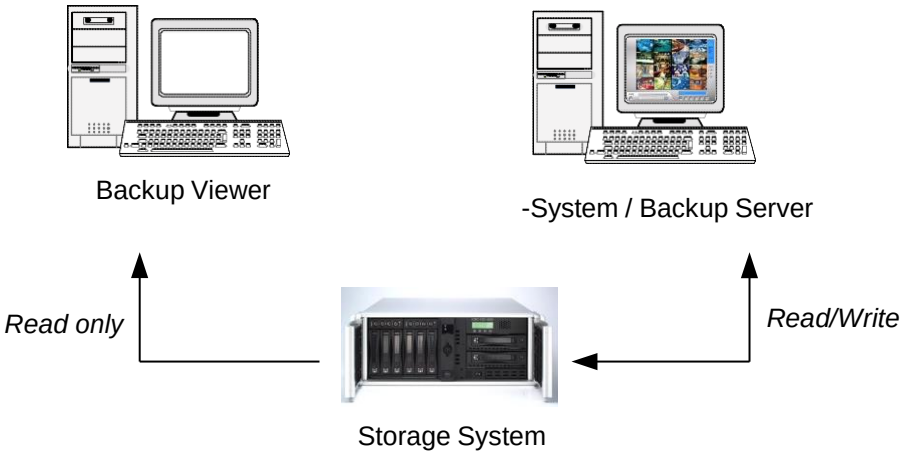


Figure 11-52

11.9.1 Usage Requirements

You must meet the following requirements when building the Backup Viewer and creating the account on the storage system:

- ⌘ The Backup Viewer is not appropriate to be installed on the computer of Backup Server (-System) due to node/host name conflict.
- ⌘ Create an account of “Read-Only” on the storage system for Backup Viewer.
- ⌘ Build the connection between the storage system and Backup Viewer. Certain storage systems may require you to install and configure additional program, e.g. iSCSI Initiator, on the computer of Backup Viewer for building the connection. Consult the documentation of the storage system for building connection with another computer.

11.9.2 Starting Backup Viewer

Before you start Backup Viewer, ensure to meet the usage requirements mentioned earlier.

1. Insert the Software DVD, click **Install Sting Alarm Supplemental Utilities**, select **-Backup Viewer** and follow the onscreen instructions.
2. Run **Backup Viewer**. The Backup Viewer window (Figure 11-51) appears.
3. Click the **Connect** button on the toolbar to enable connecting Backup Viewer to the storage system.

Note: When installing Backup Viewer on Windows 7 / 8 / Server 2012 using Typical Installation, a message will pop up to notify that Microsoft iSCSI Initiator cannot be installed, because Windows 7 / 8 / Server 2012 comes with built-in iSCSI Initiator. You can simply ignore the message and proceed with installation.

11.9.3 Performing Queries

On the iSCSI tab, you can search events or log data stored on the connected storage system.

This feature shares the same GUI and functions with the Event List Query function on WebCam Server. For details, see *Event List Query* in Chapter 8.

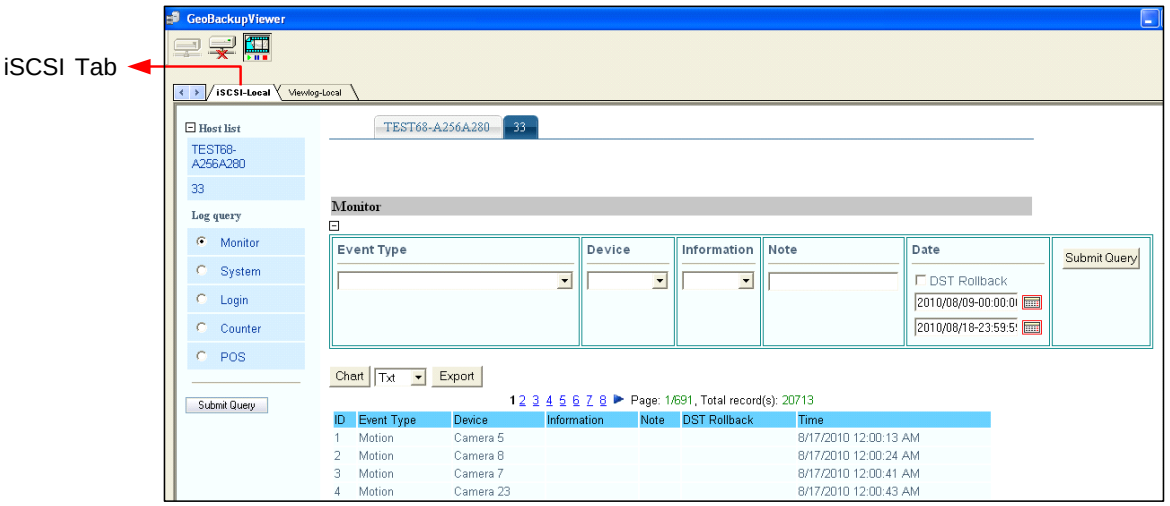


Figure 11-53

11.9.4 Viewing the Event Files

On the ViewLog tab, you can retrieve the recordings from the storage system and play video back.

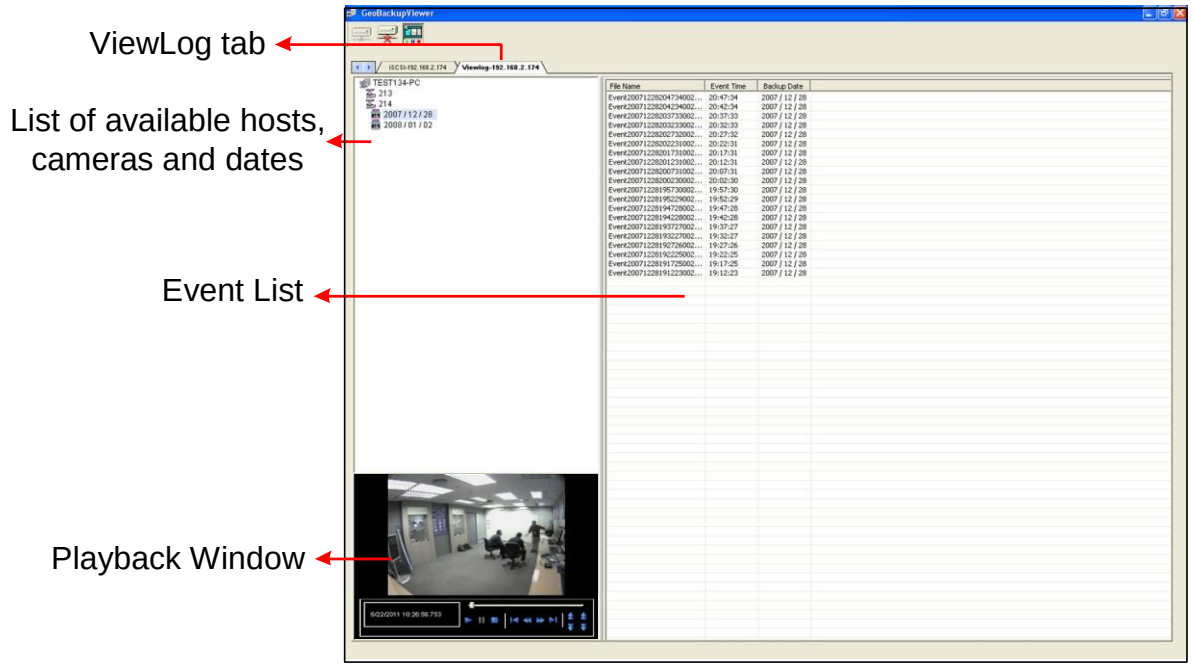


Figure 11-54

Right-clicking the playback window can change the play mode and create special effects when you play video back. For details, see *Single Player* in Chapter 4.

11.9.5 Using Remote ViewLog

Using the Remote ViewLog function, you can access the data on the -System. Click the **Remote ViewLog** button on the toolbar. The Connect to Remote ViewLog Service dialog box appears. Type the IP address, ID and Password of the -System, select **DVR** in the Host Type field, and click **Connect** to enable connecting to the -System.

11.10 Bandwidth Control Application

The Bandwidth Control is an independent application that controls and monitors the network traffic of the WebCam servers. Its features include:

- ⌘ Manage up to 10 WebCam servers
- ⌘ Get bandwidth usages of every Webcam server and every user
- ⌘ Set bandwidth thresholds for specific users and IP addresses
- ⌘ IP black and white list
- ⌘ Kick unwanted users

Note: The Bandwidth Control application only works on Internet Explorer. If the user logs in the WebCam server using other browsers, e.g. Netscape and FireFox, the Bandwidth Control cannot detect and manage the login user. However, the user of other browsers has access to JEPG and live images only.

11.10.1 Installing the Bandwidth Control

1. On the computer you want to install the Bandwidth Control program, insert the Software DVD, click **Install Sting Alarm Supplemental Utilities**, select **-Bandwidth Control Client Site**, and follow the onscreen instructions.
2. After the installation is complete, double-click the **Bandwidth Remote Control** icon created on the desktop. The Bandwidth Control window appears.

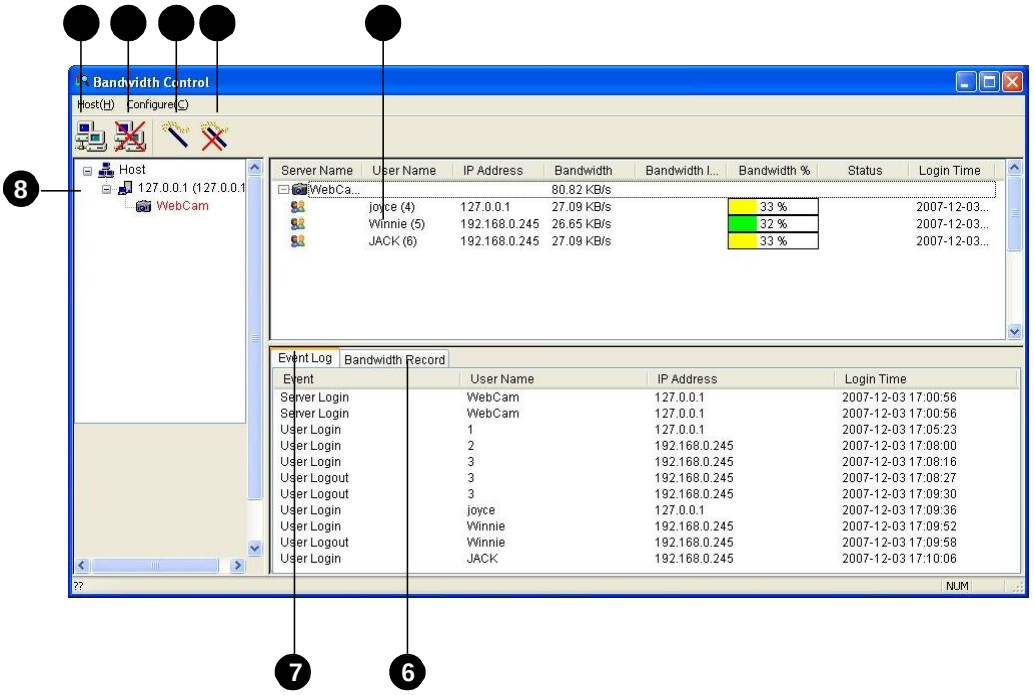


Figure 11-55

No.	Name	Description
1	Connection	Builds the connection to a WebCam server.
2	Disconnect	Stops the connection to a WebCam server.
3	Get Control	Obtains the right to remotely control the WebCam servers.
4	Give Up Control	Ceases controlling the WebCam servers and users.
5	User List	Displays the connected users and their status
6	Bandwidth Record	Displays the network traffic in graph display.
7	Event Log	Records activities of WebCam servers and users.
8	Host List	Displays all WebCam servers to be connected.

11.10.2 Allowing Remote Control at DVR

The network traffic of WebCam server can be controlled when the DVR permits the remote control from the Bandwidth Control program by the following steps:

1. Click the **Network** button (No.11, Figure 1-2), and select **WebCam Server**.
2. On the General tab, select the **Run Bandwidth Control server** option. When this option is enabled, on the Control Center Server option list, the “Bandwidth Control Service” is marked with a check.

11.10.3 Connecting to a WebCam Server

1. Click **Host** on the menu bar, and select **Connection**. Or you can click the **Connection** button on the toolbar. This dialog box appears.

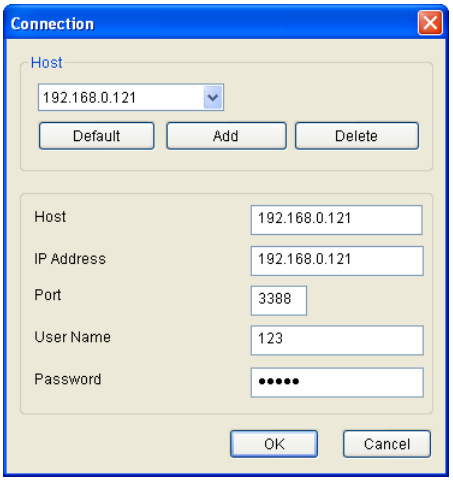


Figure 11-56

2. To add a WebCam server to be connected to, click **Add**.
3. Type host name, IP addresses, user name and password of the WebCam server. Modify the port if necessary.
4. Click **OK**. If the connection is established, the WebCam server shows up in the Host List.
5. You can add up to 10 WebCam servers by repeating above steps.
6. To stop the connection, select the host and click the **Disconnect** button.
7. Up to 5 users of the Bandwidth Control programs can connect to a single WebCam server for network traffic monitoring. However, only one user has access to bandwidth settings. When this user clicks the **Give Up Control** button, the user no longer controls the WebCam server. Whoever clicks the **Get Contro**l button first has access to bandwidth settings. For bandwidth settings, see *Controlling a WebCam Server* later in this chapter.

11.10.4 Controlling a WebCam Server

To disconnect a login user or set the bandwidth limit for a user, right-click the user to have these options:

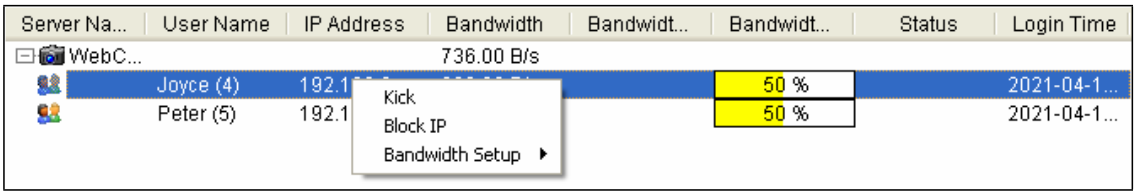


Figure 11-57

④ **Kick:** Disconnects the user from the WebCam server.

④ **Block IP:** Prohibits the IP address from connecting to the WebCam server. To use the function, the **Enable IP Black List** option (Figure 11-60) must be selected first.

④ **Bandwidth Setup:** Select **By Username** to specify a bandwidth limit for the user, or select **By IP** to limit the bandwidth used by the IP address. A setup dialog box will appear. In this example, an IP address is selected for bandwidth limit setup. Select **Bandwidth Setup**, specify a bandwidth limit, and then click **OK**.

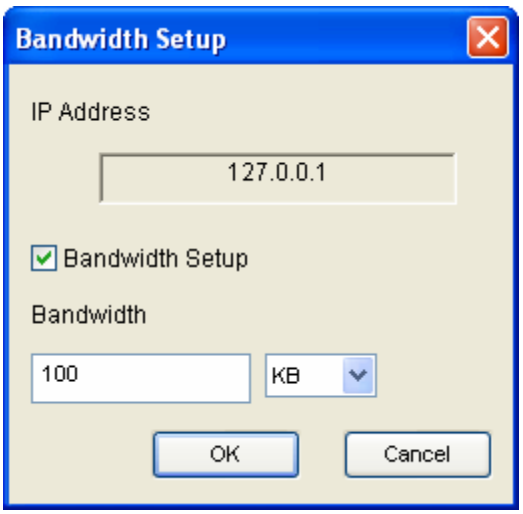


Figure 11-58

11.10.5 Bandwidth Setup

You can specify the total bandwidth allocated to a WebCam server. You can also specify the bandwidth for certain users and IP addresses. This is especially useful when your network is busy or heavily loaded.

1. Click **Configure** on the menu bar, and select **Bandwidth Setup**. A dialog box prompts for you to select a host.
2. Select the desired WebCam server, and click **OK**. This dialog box appears.

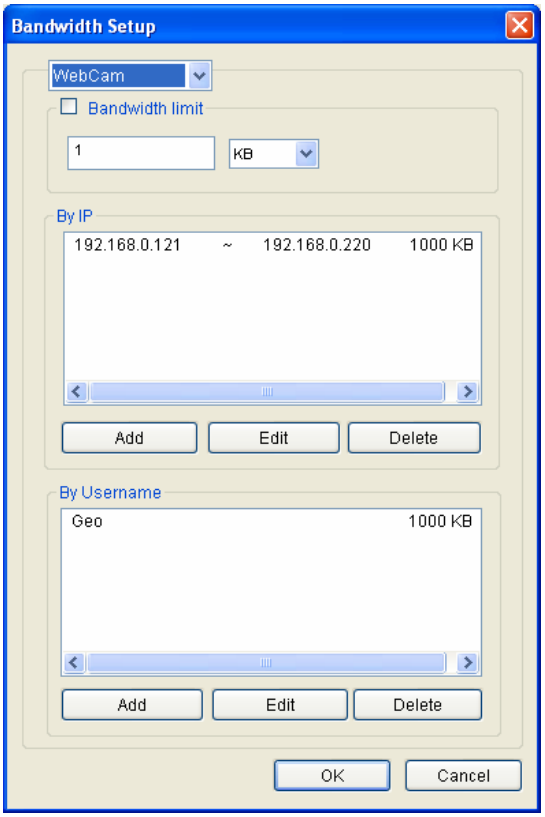


Figure 11-59

④ **Bandwidth limit:** Select this option, and define the total bandwidth that the WebCam server will be allowed to use on your network.

④ **By IP:** Click the **Add** button, and specify a specific IP address or a range of IP addresses and its bandwidth limit.

④ **By Username:** Click the **Add** button, and specify the user name and its bandwidth limit.

Note: If you have already specified the total bandwidth to a WebCam server, it is prioritized before the bandwidth limits set to user names and IP addresses.

11.10.6 Block List Setup

Two types of block lists are provided to restrict access to a WebCam server: permitting and denying a specified range of IP address to establish the connection. Note that only one type of block list can be used at one time.

1. Click **Configure** on the menu bar, and select **IP White / Black List Setup**. A dialog box prompts for you to select a host.
2. Select the desired WebCam server, and click **OK**. This dialog box appears.

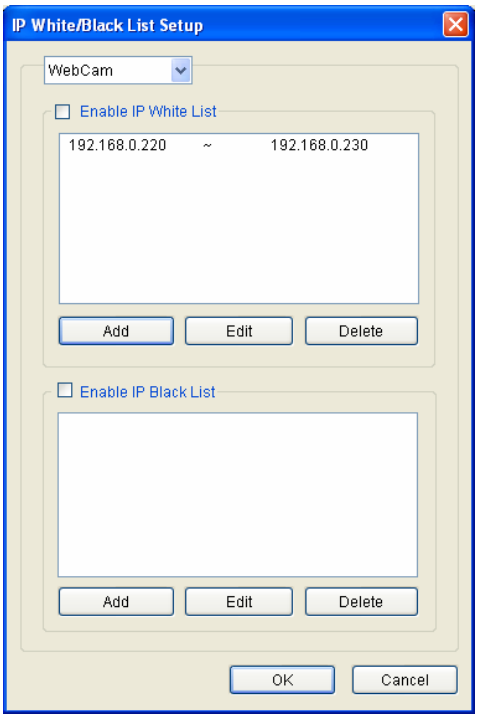


Figure 11-60

3. Select the type of block list you want to use, and click **Add** to define the IP addresses.
   ④ **Enable IP White list:** Allows the defined range of IP addresses to establish the connection.
   ④ **Enable IP Black list:** Prohibits the defined range of IP addresses from establishing the connection.
4. Click **OK** to apply the settings.

11.10.7 General Setup

You can set up sound alarm when a user logs in, or change the real-time graph display of network traffic. Click **Configure** on the menu bar and select **General Setup**. This dialog box appears.

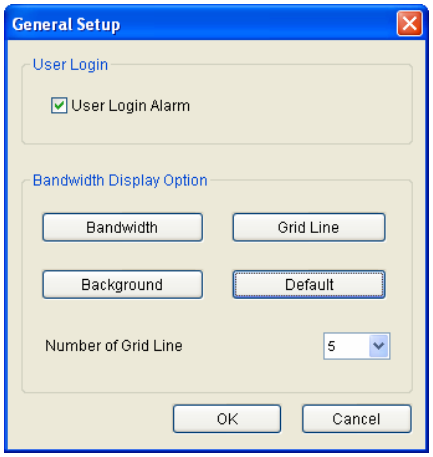


Figure 11-61

④ **User Login Alarm:** Computer alarm sounds on when a user logs in.

④ **Bandwidth:** Sets the color of bandwidth wave.

④ **Grid Line:** Sets the color of the grid lines of graph.

④ **Background:** Sets the background color of the graph.

④ **Default:** Sets the color of graph display at default.

④ **Number of Grid Line:** Use the drop-down list to select how many grid lines to be displayed.

When you click the **Bandwidth Record** tab in the Bandwidth Control window, you can view the network traffic in graph.

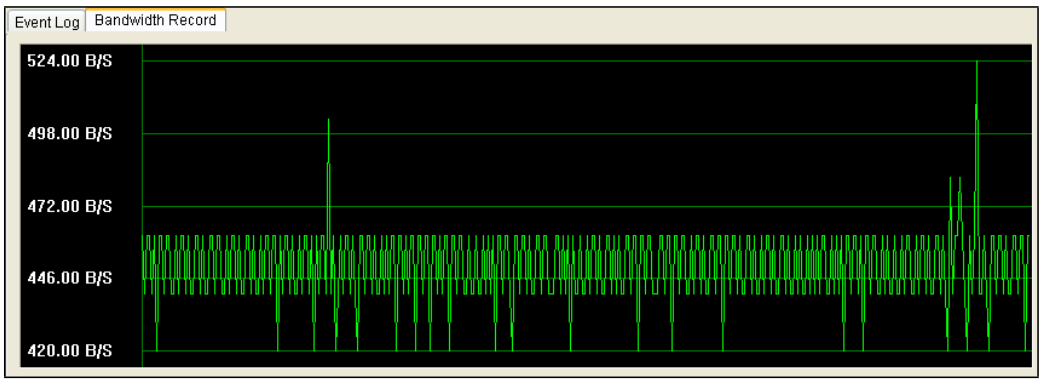


Figure 11-62

11.11 Report Generator

With the Report Generator, you can generate a daily or weekly report based on the specified recording data. The report can be either generated manually or automatically by schedule. The report is available in two types of formats: MDB and HTML. You can save the report on the hard disk, send it to a specified e-mail address or have it to be dealt in both ways. If the reports indicate the video recordings of events, you can play them back via Internet connection.

11.11.1 Starting Report Generator

1. The Report Generator program is included in the installation of Main System. Double-click **ReportGenerator.exe** from the folder.
2. The program will be minimized to the system tray. Double-click the icon to run the program.
3. Type the ID and password of the -System when you are prompted to log in.

11.11.2 Setting Report Generator

In the Report Generator dialog box, click the **Advanced Setting** tab.

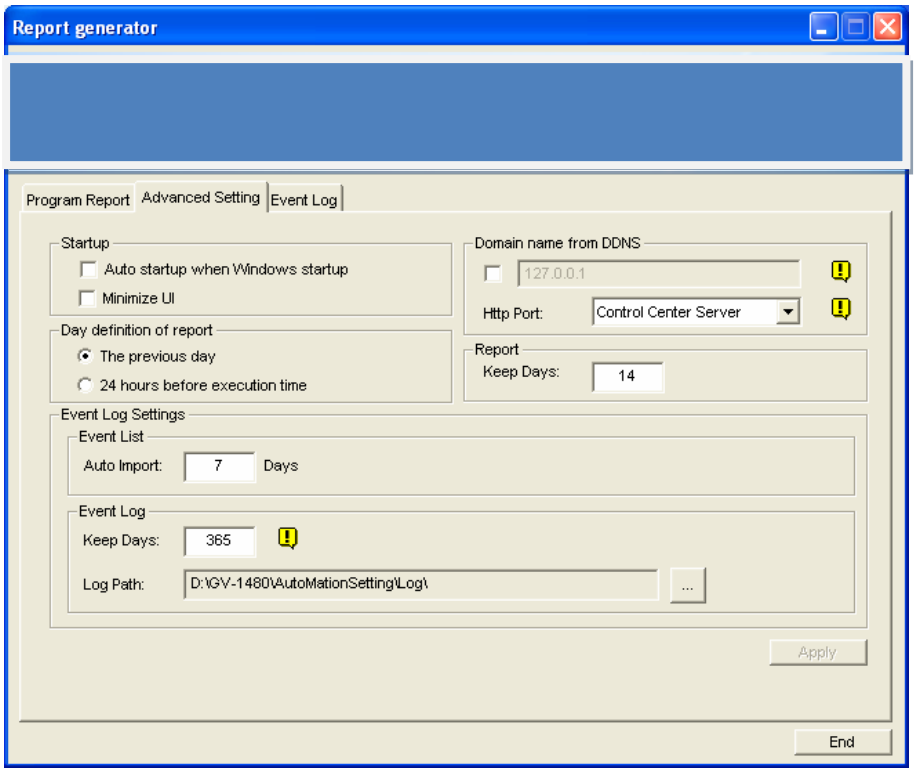


Figure 11-63

[Startup]

④ **Auto startup when Windows startup:** Select this option to start Report Generator automatically at Windows startup.

④ **Minimize UI:** Select this option to minimize the Report Generator after it is started.

[Day Definition of Report] Define the time period of data to be included in the report.

④ **The previous day:** The report is generated on the previous day's data.

④ **24 hours before execution time:** The report is generated on the data from 24 hours before report generation.

[Report]

④ **Keep Days:** If you generate reports to the hard disk, specify the number of days to keep the report files. Up to 30 days of files can be kept. To generate reports to the hard disk, see Step 4 in *Setting Report Criteria* later in this chapter.

[Domain name from DDNS] This option will generate URL links in the exported HTML report for remote video playback. For this function to work, enter the fixed IP address or domain name of the -System, and enable **Remote ViewLog Service** on the -System. To obtain a domain name, see *Dynamic DNS* earlier in this chapter. For details on remote playback, see *Playing Back Video Recordings* later in this chapter.

[Event Log Settings]

④ **Auto Import:** Specify the number of days of Report Generator logs to be displayed when the Event Log is started. Up to seven days of data can be displayed.

④ **Keep Days:** Specify the number of days to keep Report Generator logs. The logs can be kept for up to 365 days.

④ **Log Path:** Select the location to store Report Generator logs.

11.11.3 Setting Report Criteria

You can create up to 300 reports (Jobs) with different criteria.

1. In the Report Generator dialog box, click the **Program Report** tab.

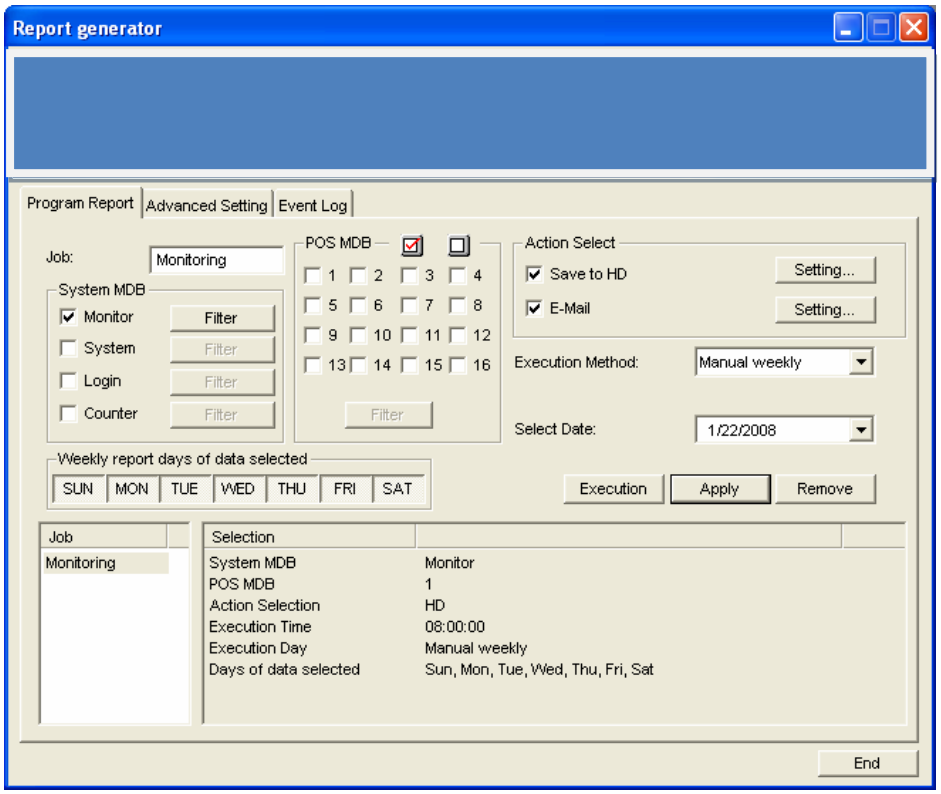


Figure 11-64

2. In the Job field, type a descriptive name for the report.
3. Select the types of events you want to include in the report. To set up specific criteria, click the **Filter** button beside each option.

   [System MDB]

   ④ **Monitor:** Includes the events of motion and I/O events.

   ④ **System:** Includes the events of functions enabled and disabled in -System.

   ④ **Login:** Includes the events of who has logged in and out of -System and WebCam Server at what time.

   ④ **Counter:** Includes the events of and result of -System's counter function.

   [POS MDB] Select the cameras for searching POS event.

4. In the Action Select field, select how the report is accessed.

   ④ **Save to HD:** Select this option to save the report on the hard disk. Click the **Setting** button to display this dialog box.

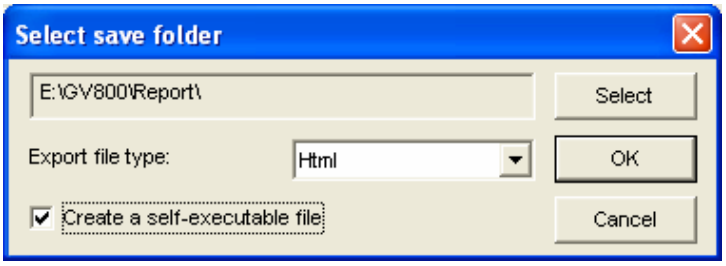


Figure 11-65

   Click **Select** to specify the storage location, and use the drop-down list to select a report format. If you want to create a self-executable file of the report, select **Create a self-executable file**.

   ④ **E-Mail:** Select this option to send the report to an e-mail address as an attachment. Click the **Setting** button to set up the e-mail account and attachment.

   For details on setting up the e-mail account, see *Setting Email Server* in Chapter 1.

   For details on setting up the attachment, see *E-Mail Attachment Settings* later in this chapter.

5. In the Execution Method drop-down list, choose the way and time to generate the report.

   ④ **Everyday:** Automatically generates daily reports at a specific time. Specify the time by using the **Select Time** drop-down list.

   ④ **Sun - Sat:** Automatically generates reports on the selected day (Sun to Sat) and at a specific time. Specify the time by using the **Select Time** drop-down list.

   To select the days of data to be included in the report, click the desired day buttons.

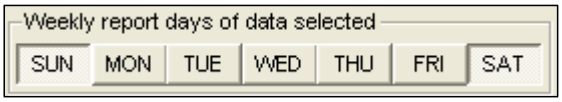


Figure 11-66

④ **Manual daily:** Manually generates a daily report.

” If you select **The Previous day** on the Advanced Setting tab (Figure 11-63), the report will be generated on the data of one day before your specified date. For example, you enter “12/10/2007” in the **Select Date** drop-down list. The report is generated on the data of 9th December 2007.

” If you select **24 hours before execution time** on the Advanced Setting tab (Figure 11-63), the report will be generated on the data of 24 hours before your specified date and time. Specify the date and time by using the **Select Date** and **Select Time** drop-down lists.

④ **Manual Weekly:** Manually generates a weekly report.

” If you select **The Previous day** on the Advanced Setting tab (Figure 11-63), the generated report will contain the data of 7 days before your specified date. For example, you enter “12/10/2007” in the **Select Date** drop-down list. The report is generated on the date from December 3rd to 9th in 2007.

To select the days of data to be included in the report, click the desired day buttons. See Figure 11-66.

” If you select **24 hours before execution time** on the Advanced Setting tab (Figure 11-63), the generated report will contain the data of 7 days counting back on your specified date and time. Specify the date and time by using the **Select Date** and **Select Time** drop-down lists. For example, if you enter “12/10/2007” and “01:00”, the report is generated on the time from 01:00 am, December 10th to 01:00 am, December 4th, 2007.

To select the days of data to be included in the report, click the desired day buttons. See Figure 11-72.

11.11.4 E-Mail Attachment Settings

After you set up the e-mail account to receive the reports as e-mail attachments, you can also set up the attachment limits to avoid sending out large files.

1. On the Program Report tab, select **E-mail** and click the **Setting** button beside. This dialog box appears.

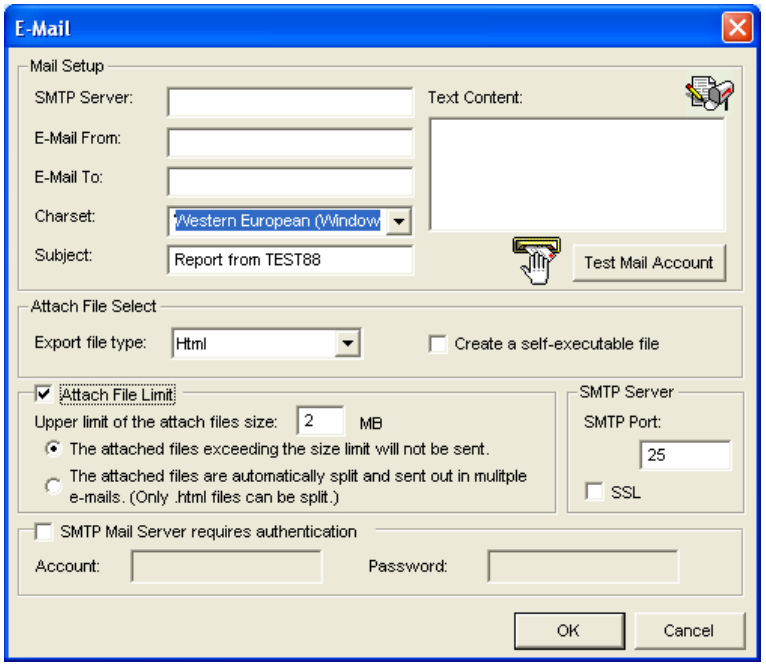


Figure 11-67

2. In the Attach File Select field, use the **Export file type** drop-down list to select Html or MDB as a file format. If you want to create a self-executable file of the report, select **Create a self-executable file**.
3. Select **Attach File Limit**, and decide the size limit of the attached file. Set the limit between 1 MB and 10 MB.
4. Select one of these options to set the attachment condition.

   ④ **The attached files exceeding the size limit will not be sent:** When the attached report file exceeds the size limit, the e-mail will not be sent.

   ④ **The attached files are automatically split and sent out in multiple e-mails:** If the attached file exceeds the size limit, it will be automatically split and sent out in multiple e-mails. Note this option cannot apply to the report files in .mdb format.

For details on setting Mail Server, see *Setting Email Server* in Chapter 1.

11.11.5 Playing Back Video Recordings

In a HTML format report, the video recordings can be played back with the Remote ViewLog function. Ensure the **Remote ViewLog Service** is enabled on the -System that owns those recordings.

1. Open a report and click the desired video icon.

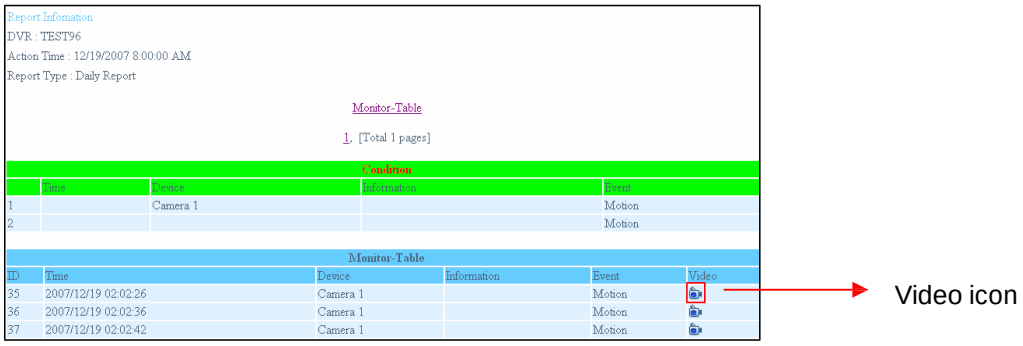


Figure 11-68

2. If the **Domain name from DDNS** option on the Advanced Setting tab (Figure 11-63) is not selected, this dialog box will appear.

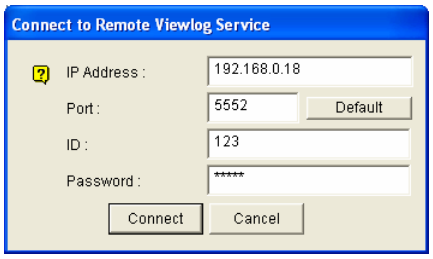


Figure 11-69

3. Type the IP or domain name, ID and password of the -System, and then click Connect for playback.

Figure 11-70

4. You can change the play mode and create special effects on the video by right-clicking on the playback window. For details on the playback window, see *Single Player* in Chapter 4.

11.11.6 Viewing Event Log

All Report Generator events are recorded to the event log. To view the event log, in the Report Generator dialog box, click the **Event Log** tab. All events are displayed in descending order.

For the related settings of the event log, see *Event Log Settings* in *Setting Up Report Generator* earlier in this chapter.

11.12 Spot Monitor Controller

-Combo Card (-1120 / 1280 / 1480) and **-Combo A Card** (-1120A / 1280A / 1480 A) come equipped with a TV output allowing you to connect one spot monitor or TV monitor to the computer. With the Spot Monitor Controller, you can define the screen divisions, set the channel sequence of each scanned page and adjust video images on the additional monitor.

11.12.1 Spot Monitor Controller

To start the Spot Monitor Controller, follow these steps:

1. Click the **Configure** button (No. 14, Figure 1-2), select **Accessories**, select **DSP Spot Monitor**, and select **Spot Monitor Setup**. This dialog box appears.

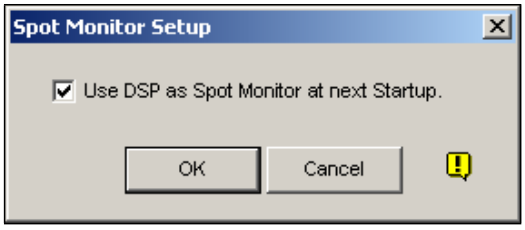


Figure 11-71

2. Select **Use DSP as Spot Monitor at next Startup**, and click **OK**.
3. Restart the -System.
4. Click the **Configure** button (No. 14, Figure 1-2), select **Accessories**, select **DSP Spot Monitor**, and select **Spot Monitor Controller**. The Spot Monitor Controller window appears.

Note: When the DSP Spot Monitor Control feature is enabled, DSP Overlay will be disabled in the Main System.

[Advanced Layout]

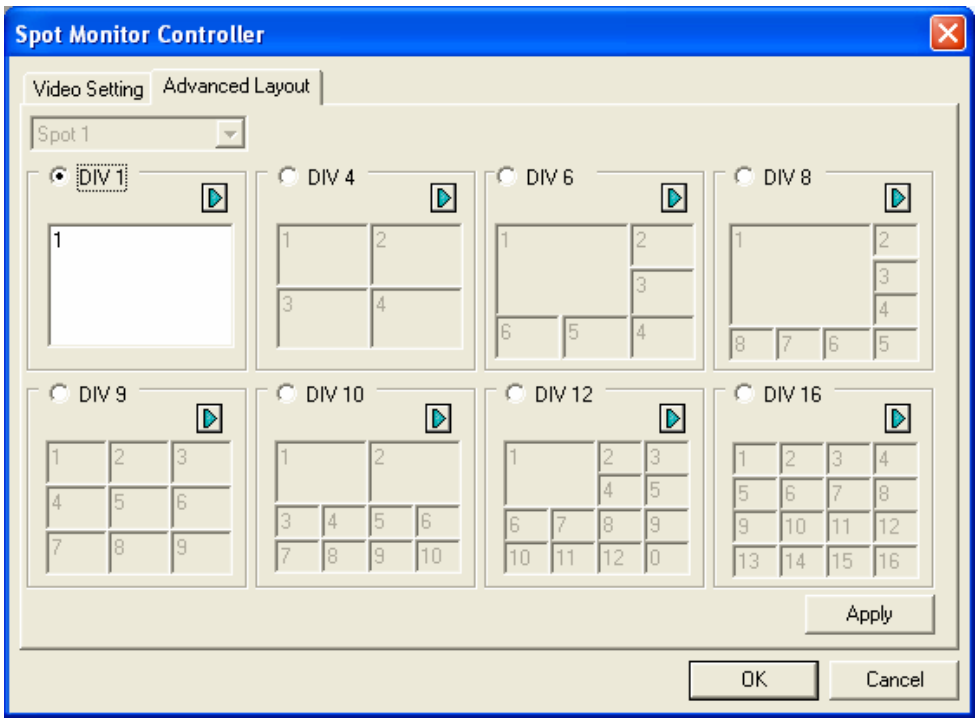


Figure 11-72 *Spot Monitor Controller*

④ **Spot x:** The drop-down list is available when the -System is equipped with two video capture cards and connects two additional monitors. Select **Spot 1** to configure the screen display on the first monitor, and **Spot 2** for the second monitor.

④ **DIV 1-16:** Screen division option.

④ **Right Arrow button:** Sets the channel sequence of each scanned page. Up to 16 scanned pages can be configured. Click the button to display this dialog box.

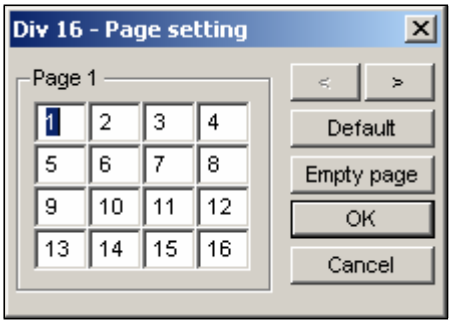


Figure 11-73 *Page Setting*

” **Screen Division:** Displays the channel sequence. You can modify the sequence by typing the number directly on each division.

” **< > buttons:** Navigate pages.

” **Empty page:** Clears up the channel sequence of the open page.

[Video Setting]

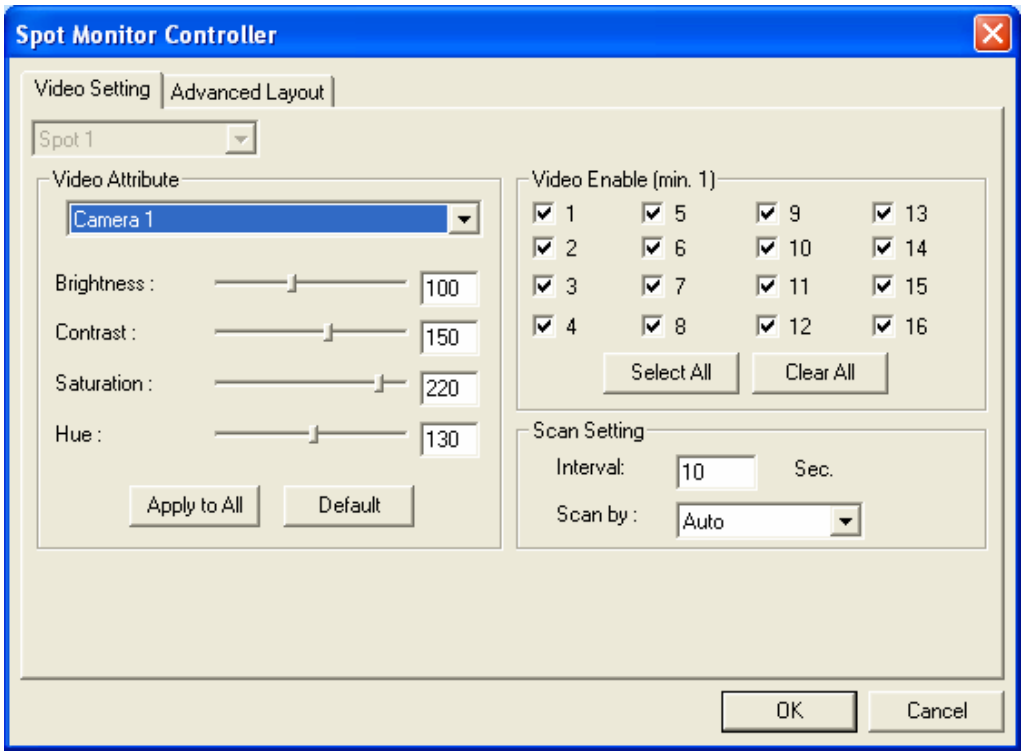


Figure 11-74

[Spot X] See the same option in the **Advanced Layout** tab.

[Video Attribute] Select a desired camera from the drop-down list to adjust image attributes, such as Brightness, Contrast, Hue and Saturation.

[Video Enable] Select the desired cameras for display on another monitor.

[Scan Setting] Enter the interval between the scanned pages. Select **Auto** if you want to automatically scan the cameras or **Manual** to scan at your own speed.

11.12.2 Spot Monitor Panel

With the Spot Monitor Panel, you can switch screen divisions and channels as well as starting and stopping page scan immediately. On the Main System, click the **TV-Out** button . This panel appears.

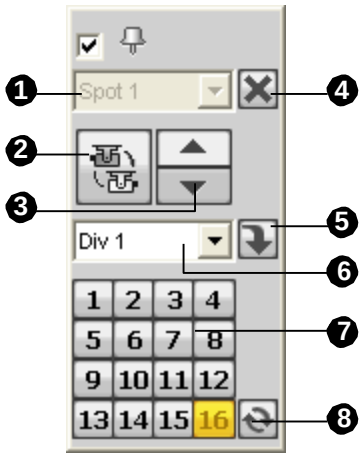


Figure 11-75

The controls on the DSP Spot Monitor Panel:

No.	Name	Description
1	Spot x	**Spot 1** is for screen display on the first monitor, and **Spot 2** for that on the second monitor.
2	Scan	Automatically or manually rotates channels and stops rotation.
3	Previous Page	Goes to the pervious page of the scanned pages.
4	Next Page	Goes to the next page of the scanned pages.
5	Exit	Closes the Spot Monitor Panel.
7	Switch	Opens or closes the channel menu.
8	Channel Menu	Displays the desired channel for single view.
9	Screen Division	Sets screen divisions to 1, 4, 6, 8, 9, 10, 12 and 16.
10	Zoom Esc	After single view, click this button to restore the first scanned page, but restore the last channel when the screen division is set to 1.

11.13 Quad Spot Monitor Controller

The Controller integrates the -Multi Quad Card with TV monitor (spot monitor) applications. It features:

⌘ Up to 5 TV monitors can be controlled.

⌘ TV Monitor 1 supports up to 16 screen divisions, and TV Monitor 2 to TV Monitor 5 support 1 and 4 divisions.

⌘ Different screen divisions can be set up on each monitor.

⌘ The channel sequence of screen divisions is user-defined.

Note:

1. This function is only supported in -Video Capture Cards with -Multi Quad Card, which include -600A / 650A / 800A / 1120A / 1240A / -1480A.
2. The Controller does not support the videos from IP devices. To export videos from IP devices, refer to the *Digital Matrix* section later in this chapter.

11.13.1 Setting the Controller

Click the **Configure** button (No. 14, Figure 1-2), point to **Accessories**, and select **Quad Spot Monitors Setup**. The TV Quad Setting dialog box appears.

⌘ In the General Setting tab, you can modify Video Format and Video Attribute for all TV monitors.

⌘ In the TV tabs (TV1 to TV5), you can set up the following configurations for each TV monitor.

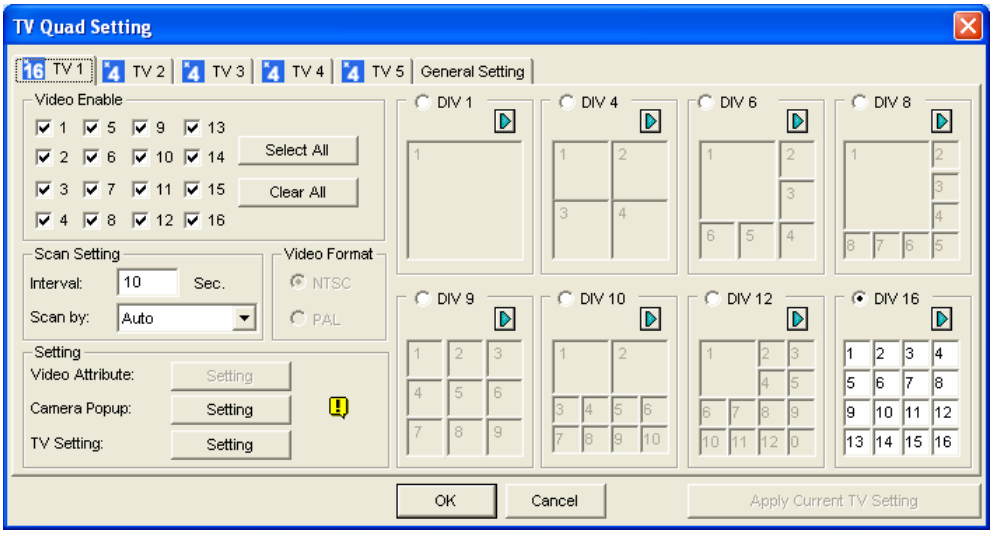


Figure 11-76

[Video Enable] Check or uncheck the desired channels displayed on monitor screen.

[Scan Setting]

④ **Interval:** Enter the interval between the scanned pages (see Figure 11-74 for the scanned page). Set the time between 1 and 999 seconds.

④ **Scan by:** Select **Auto** to scan the channels automatically or **Manual** to scan at your speed.

[Setting]

④ **Camera Popup:** See *Setting Pop-up Views* below.

④ **TV Setting:** Click the **Setting** button to display this dialog box.

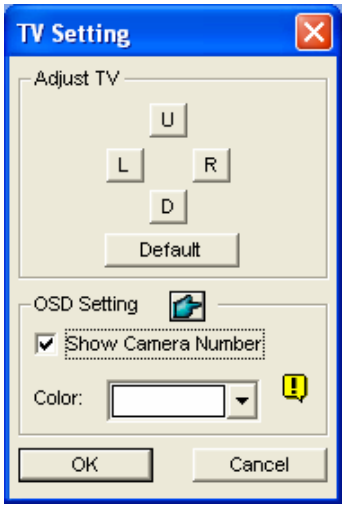


Figure 11-77

Press the 4 direction buttons (**U**, **L**, **R** and **D**) to adjust the positions of the divisions on the monitor screen.

To display the camera number on the TV monitor, check the **Show Camera Number** option. To display the camera numbers on all connected TV monitors, check the **Show Camera Number** option, and then click the finger button.

To change the color of the camera number indicator on the TV monitor, use the Color drop-down list to select the desired color.

[DIV 1-16] In the TV Quad Setting window (Figure 11-76), there are screen division options. You can modify the channel sequence by typing the number directly on each division. Click **OK** or **Apply Current TV Setting** to apply your configurations.

④ **Right Arrow Button:** Sets the channel sequence of each scanned page. Click the arrow button to display this dialog box.

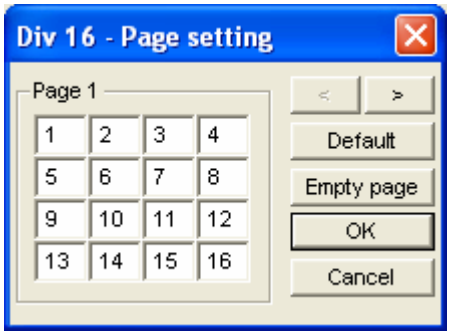


Figure 11-78

- **Screen Division:** Displays the channel sequence. You can modify the sequence by typing the number directly on each division.
- **< > Buttons:** Navigates pages.
- **Empty page:** Clears up the channel sequence on the open page.

11.13.2 Setting Pop-up Views

The pop-up camera views on the screen notify users of the current event, whether it is motion or I/O devices being triggered. You can decide to have pop-up cameras on computer screen, TV monitor or both together.

Activating Pop-up Views

1. In the TV Quad Setting window, click the desired TV tab.
2. Click the **Setting** button of Camera Popup. This dialog box appears.

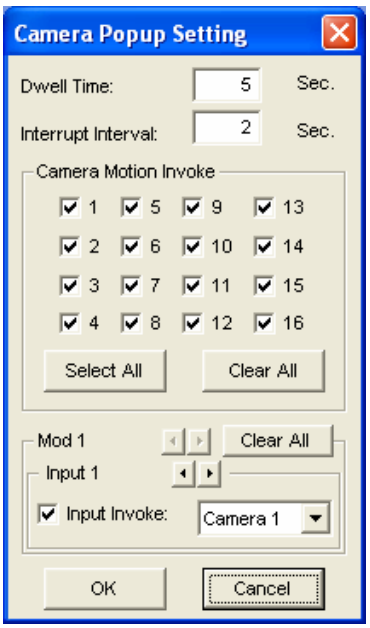


Figure 11-79

3. Set the Dwell Time and Interrupt Interval.
   - ④ **Dwell Time:** Specify the amount of time a pop-up view remains on the monitor screen when an event occurs. Set the dwell time between 1 and 120 seconds.
   - ④ **Interrupt Interval:** Specify the interval between pop-up views when events occur. Set the time interval between 1 and 60 seconds.
4. To be alarmed with a pop-up view whenever movement occurs in the video image, select the desired cameras to be popped up in the Camera Motion Invoke section.
5. To be alarmed with a pop-up view when input devices are triggered, select input module and use the drop-down list to select the desired camera to be popped up.
6. Click **OK** to apply the settings.

Tip: All cameras can be repetitively setup on different TV monitors. If one camera is selected on more than one TV monitors, it can be set with different alert events.

11.13.3 Displaying TV Quad Panel

On the main screen, click the **TV-Out** button This panel will appear.

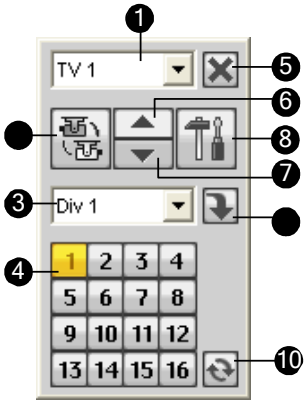


Figure 11-80

The controls on the TV Quad Panel:

No.	Name	Description
1	Monitor	Selects the monitor to be controlled.
2	Scan	Automatically or manually rotates channels, and stops rotation.
3	Screen Division	Sets screen divisions. Only TV 1 can support screen divisions up to 16, and TV 2 to TV 5 supports 1 or 4 screen divisions.
4	Channel Menu	Displays the desired channel for single view.
5	Exit	Closes the TV Quad Panel.
6	Previous Page	Scans the previous page.
7	Next Page	Scans the next page.
8	Settings	Displays the TV Quad Setting window.
9	Switch	Displays or hides the channel menu.
10	Zoom Esc	After single view, click this button to return to the first scanned page or return to the last channel when the screen division is set to 1.

Note: If the DSP Spot Monitor function is enabled at the same time with the Quad Spot Monitors, the TV-Out button has two options: Spot Monitor Panel and TV Quad Panel. Select the desired panel to be displayed on the screen.

11.14 Digital Matrix

To create more screen space to display multiple channels, such as 32 channels, Digital Matrix is thus introduced to provide a way to view and manage up to 8 monitor displays.

The monitor of the computer where you configure the settings and control is called the “primary monitor” and up to 7 additional monitors can be connected with. Additional graphic cards are required to install multiple monitors. Most graphic cards now support dual monitors at least. To connect up to 8 monitors, you may need 4 graphic cards installed in the computer of -System.

The Digital Matrix includes these features:

- **Live view:** You can set different live views and screen divisions for each monitor.
- **Automatic channel scan:** You can set up to 16 scanned pages with different screen divisions and channels for each monitor.
- **Pop-up Alert:** You can be alerted by pop-up live videos when motion is detected or I/O devices are triggered.

11.14.1 Activating Multiple Monitors

Use Windows **Display Properties** to activate multiple monitors. Here we use Windows XP to illustrate the steps of configuration.

1. Right-click the desktop, click **Properties** and click the **Settings** tab. This dialog box appears.

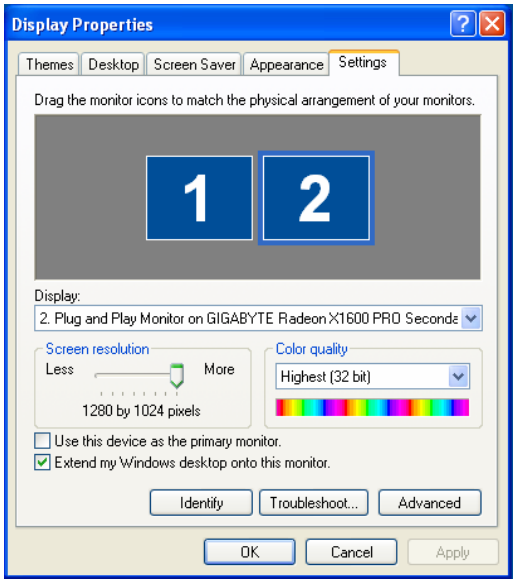


Figure 11-81

2. Click the **Display** list. If you do not see multiple monitors listed, check if your additional monitors are connected with the computer properly.
3. Select the primary monitor from the list, and select **Use This Device as the Primary Monitor**.
4. Select additional monitors from the list, and select **Extend my Windows desktop onto this monitor** for each monitor.
5. Click **Identify**. Windows XP displays a large number to identify your monitors. Drag and drop the monitor icons to match the physical arrangement of your monitors.
6. Click **OK**.
7. Start the -System, click **Configure**, click **Accessories**, select **Digital Matrix Setting**, select monitors from the **Display** list and select **Activate** for each monitor. For example, if you install 7 additional monitors, you need to activate Display 1 to Display 7 one by one.
8. Click **Apply**. Your additional monitors should now display the channels seen on the primary monitor. See the figure below for example.

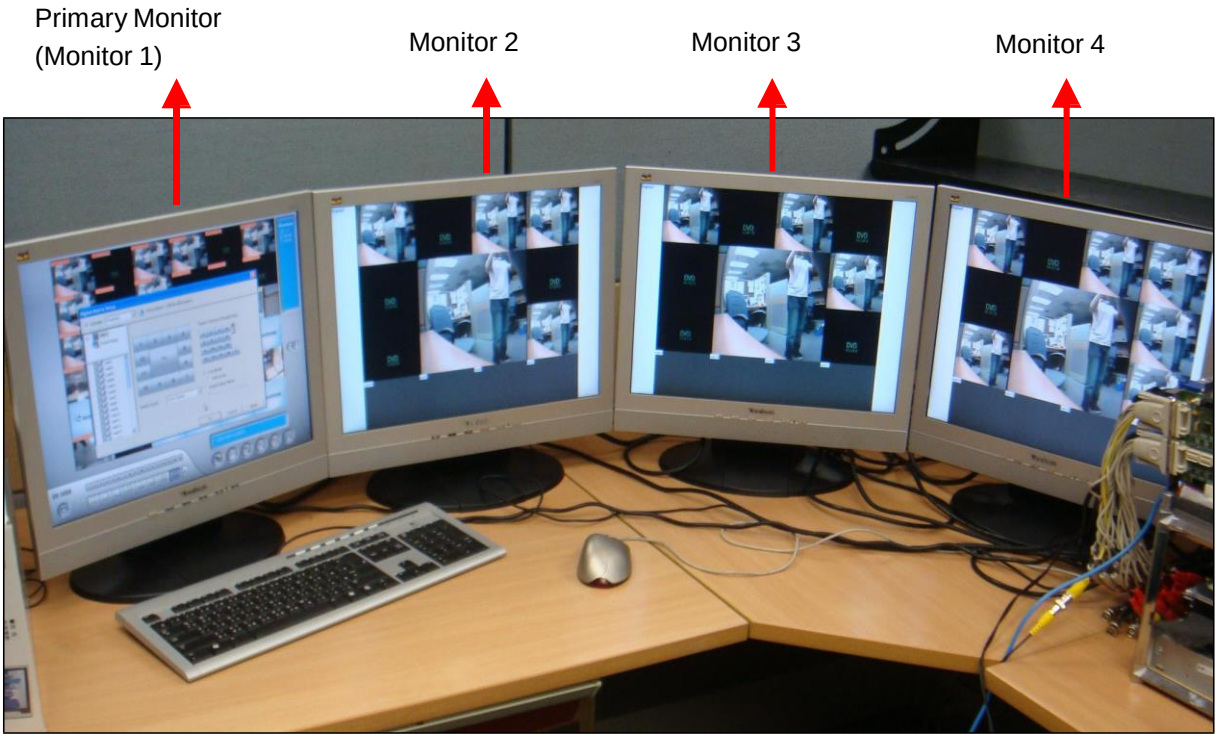


Figure 11-82

11.14.2 Setting Live View

You can set different live views and screen divisions for each monitor.

1. On the main screen, click **Configure**, click **Accessories**, and select **Digital Matrix Setting**. This dialog box appears.

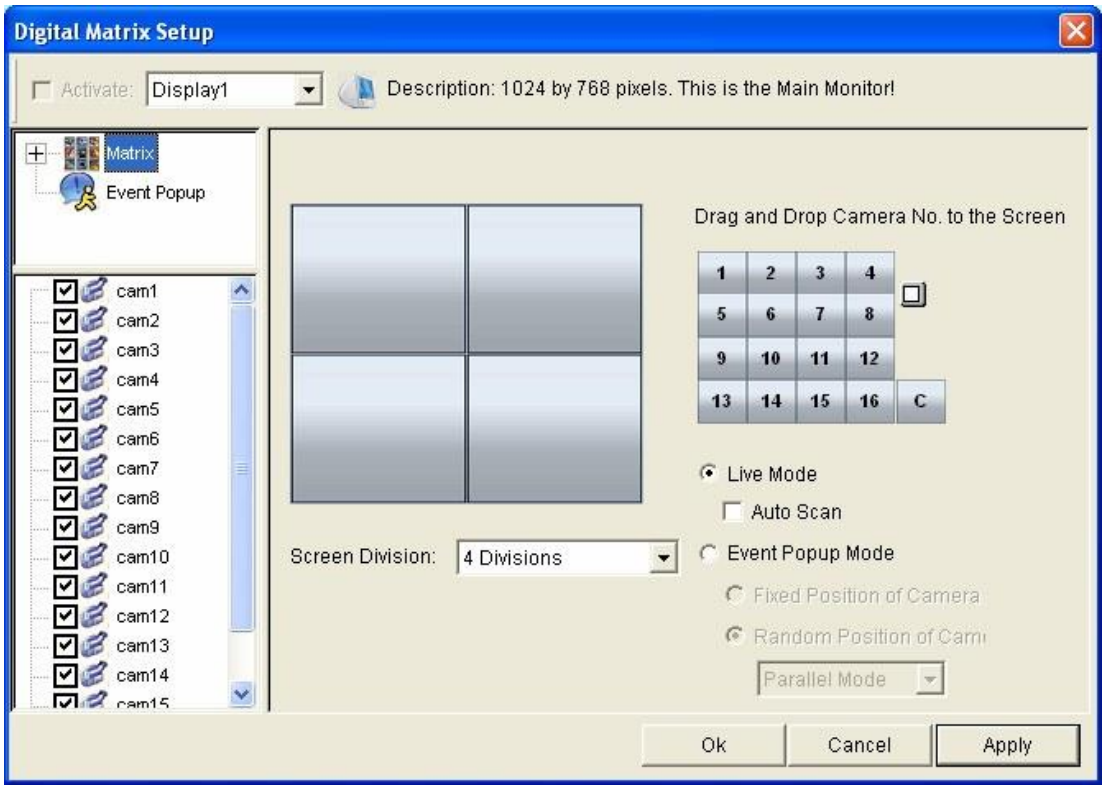


Figure 11-83

2. Use the **Display** list to select the monitor to be configured.
3. Select **Screen Division**.
4. Drag and drop the camera numbers to the desired positions on the divisions. To clear the assignment, drag and drop the “C” icon to that position.
5. Select **Live Mode**.
6. Repeat above steps to configure other monitors.
7. Click **OK** to apply the settings.

11.14.3 Setting Scanned Pages

You can set up to 16 scanned pages with different screen divisions and channels for each monitor.

1. Use the **Display** list to select the monitor to be configured.
2. In the upper-left column, expand the **Matrix** folder tree, and then click **Page 1**. This page appears.

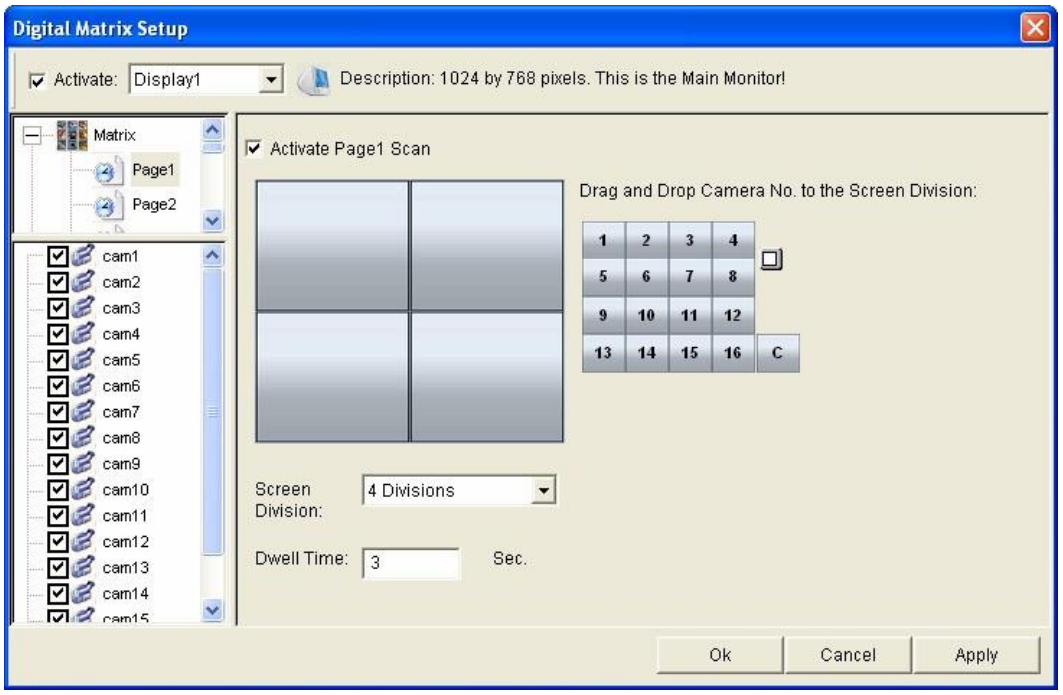


Figure 11-84

3. Select **Activate Page 1 Scan**.
4. Select **Screen Division**.
5. Drag and drop the camera numbers to the desired positions on the divisions. To clear the assignment, drag and drop the “C” icon to that position.
6. Specify **Dwell Time** for how long this scanned page remains on the monitor.
7. Repeat Steps 2 to 5 to configure more scanned pages for the specific monitor.
8. Repeat Steps 1 to 7 to configure scanned pages for other monitors.
9. In the upper-left column, click the **Matrix** icon and return to Figure 11-83.
10. Select **Auto Scan**.
11. Click **OK** to start scanning among pages.

11.14.4 Setting Pop-up Alert

You can be alerted by pop-up live videos when motion is detected or I/O devices are triggered.

1. Use the **Display** list to select the monitor to be configured.
2. In the upper-left column, click **Event Popup**. This page appears.

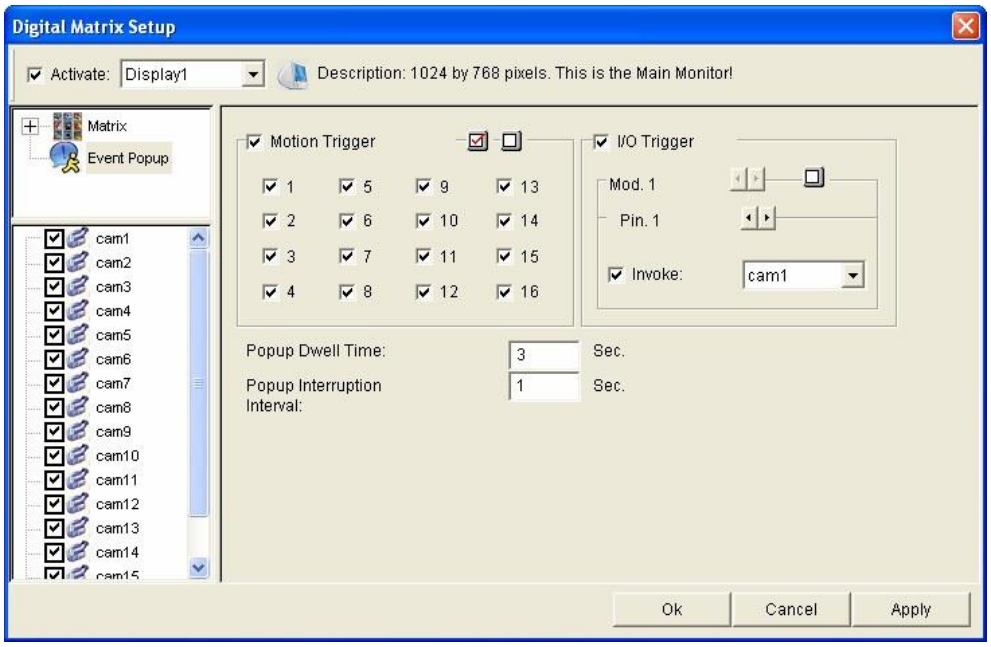


Figure 11-85

④ **Motion Trigger:** The live video of selected cameras pops up when motion is detected.

④ **I/O Trigger:** The live video of assigned camera pops up when the selected input device is triggered.

④ **Popup Dwell Time:** Specify the amount of time that a pop-up live video remains in the foreground.

④ **Popup Interruption Interval:** Specify the interval between camera pop-ups. This option is useful when several cameras are activated for pop-up alert at the same time.

3. Use the **Display** list to select other monitors for setup.
4. After above settings, click the **Matrix** icon and return to Figure 11-83.
5. Select **Event Popup Mode**. Then select **Fixed Position of Camera** or **Random Position of Camera**. For these two options, see *Setting Pop-up Positions* section below.
6. Click **OK**.

7. Start monitoring. When motion is detected or the input device is triggered, the live video will pop up for alert.

Setting Pop-up Positions

When you select **Random Position of Camera**, you can decide the positions for pop-up cameras.

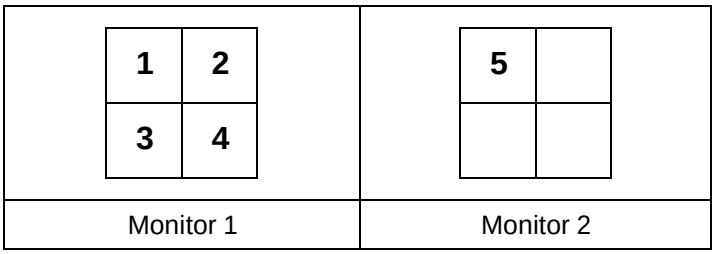
④ **Fixed Position of Camera:** The cameras pop up in their assigned positions. To assign positions, select **Screen Division**. Then drag and drop the cameras number to the desired potions on the divisions.

④ **Random Position of Camera:** The positions of pop-up cameras are based on the sequence order of triggers. There are two modes for this position:

1. **Cascade Mode:** This mode can avoid the same cameras popping up on different monitors. This is suggested to be used when multiple monitors are placed close to each other.

   Example:

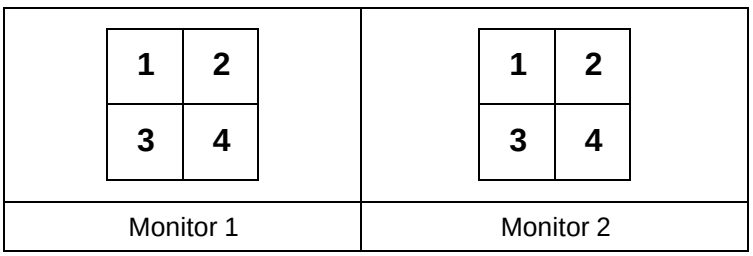
   Camera 1, Camera 2, Camera 3, Camera 4 and Camera 5 are assigned for alert popup on both Monitor 1 and Monitor 2. Monitor 1 is set at 4 screen divisions. When the five cameras are triggered at same time, the first 4 cameras show up on Monitor 1 and the 5th on Monitor 2.



2. **Parallel Mode:** This mode allows the same cameras simultaneously pop up on different monitors. This is suggested to be used when multiple monitors are placed in separate rooms.

   Example:

   Camera 1, Camera 2, Camera 3 and Camera 4 are assigned for pop-up upon motion detection on both Monitor 1 and Monitor 2. When the four cameras are triggered at the same time, they will show up simultaneously on both Monitor 1 and Monitor 2.



11.14.5 Setting Live View with Pop-up Alert

You can set a different live view mode with pop-up alert together for each monitor. When alert events occur, the live video of the associated camera will pop up on the assigned monitor to replace its live view mode.

1. To configure live view mode, follow the instructions in *Setting Live View* earlier in this chapter.
2. To configure pop-up alert, in the upper left column, click **Event Popup**. Figure 11-85 appears.
3. Configure **Motion Trigger**, **I/O Trigger**, **Popup Dwell Time** and **Popup Interruption Interval** for each monitor. For details see *Setting Pop-up Alert* earlier in this chapter.
4. Click the **Matrix** icon and return to Figure 11-83. Ensure the **Live Mode** option is selected.
5. Click **OK**. The live view mode you configured for each monitor is displayed.
6. Start monitoring. When alert events occur, the associated camera will pop up on the desired monitor.

11.14.6 Controlling Screen Display

During Digital Matrix operations of page scan or alert popup on other monitors, you can instantly suspend the predefined task on a monitor, and change its screen divisions or remain on specific channels when you spot suspicious events.

1. On the main screen, click **ViewLog** and select **Digital Matrix Channel Lock**. This dialog box appears.

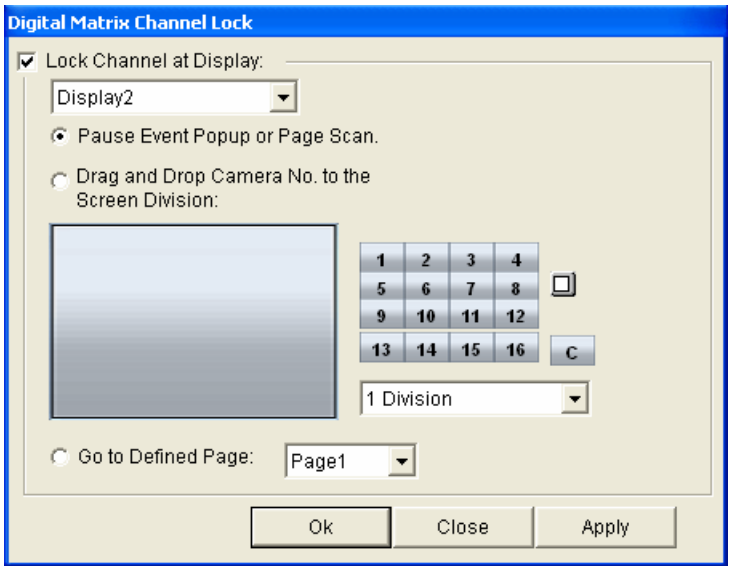


Figure 11-86

2. Use the **Display** list to select the monitor to be configured.
3. Select **Lock Channel at Display** to control the specific monitor.
4. Select one of the three options:

   ④ **Pause Event Popup or Page Scan:** Suspends alert popup and page scan operations.

   ④ **Drag and Drop Camera No. to the Screen Division:** Displays desired camera channels. Use the **Division** list to select the screen divisions. Drag and drop the camera numbers to the desired positions on the divisions. To clear the assignment, drag and drop the “C” icon to that position.

   ④ **Go to Defined Page:** Displays a specific scan page.

5. Click **Apply** or **OK** to apply the settings.

11.15 GIS Recording

-System can record the video along with GPS data of its own and the connected IP devices. With the recorded GPS data, you can view the recordings simultaneously with the GPS locations of -System and connected IP devices on Google Maps, Microsoft Virtual Earth, OpenStreetMap or self-defined maps.

If you are the user of -GIS monitoring station, the GPS data collected from either -System or from connected IP devices can also be sent to the -GIS for central monitoring.

11.15.1 Setting the GPS Receiver

To record the GPS location data of -System, -GPS USB Receiver is required to connect to the local computer. Also, you need to run the **GeoGISClient** program in the background to receive the GPS data from the GPS receiver.

1. Run **GeoGISClient.exe** from the folder. This dialog box appears.

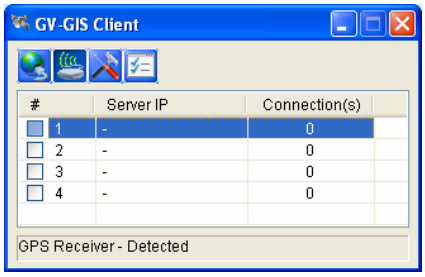


Figure 11-87

2. To add the GPS receiver to the -System, click the button and click the **GPS Receiver** tab. This dialog box appears.

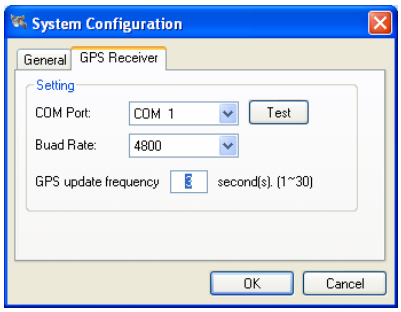


Figure 11-88

3. Select the **COM Port** the GPS receiver is connected to and click **Test** to detect the device. Select **Baud Rate** of the GPS receiver (refer to the documentation of the GPS receiver). Specify the time in seconds for the frequency to update the GPS data. Then click **OK.**
4. Click the button to start receiving GPS data from the GPS receiver.

11.15.2 Recording GPS Locations of -System

After configuring the GPS receiver on -System as mentioned earlier, you can enable the GIS function to record videos with GPS locations of -System.

1. To enable the GIS function of -System, click the **Configure** button on the main screen, select **Accessories** and select **Enable Local GIS**.
2. Start monitoring. The GPS data of -System will be recorded with the video.

11.15.3 Recording GPS Locations of the IP Device

If the connected IP device is also equipped with and enabled for the GPS function, you can choose to record videos with GPS locations of the IP device.

1. To record the GPS data of a remote IP device, ensure the GPS function on the IP device is enabled.
2. Right-click the IP device listed on the IP Device Setup window and select **GIS Setting**.
3. Select **Enable GIS Data** to receive the GPS data from the IP device.

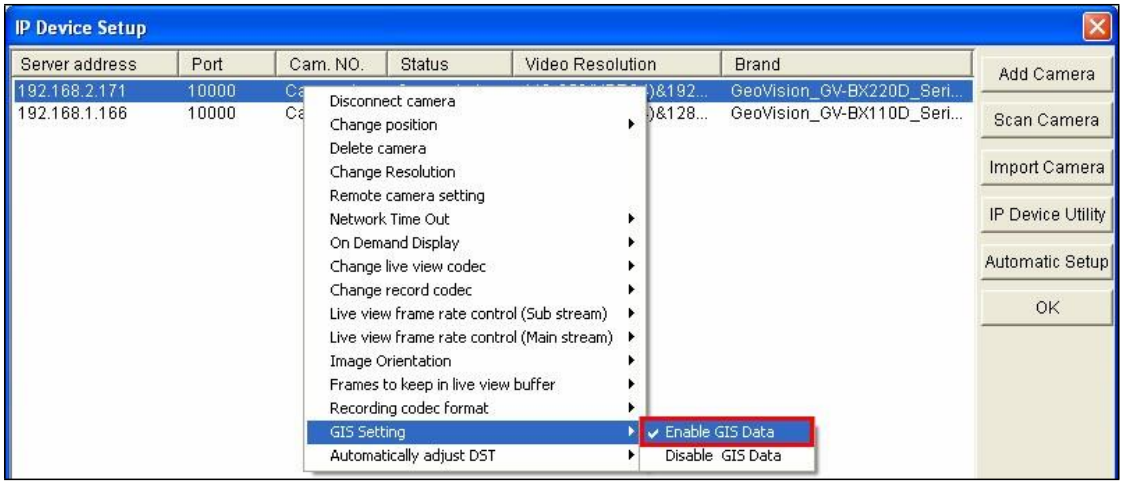


Figure 11-89

4. To enable the GIS function of -System, click the **Configure** button on the main screen, select **Accessories** and select **Enable Local GIS**.
5. Start monitoring. The GPS data of the IP device will be recorded with its own video.

Note:

1. If the GIS function of -System is not enabled at Step 4, the GPS data of the IP device will not be recorded on -System.
2. If the remote GIS function of the IP device is not enabled at Step 3, the video of the IP device will be recorded with the GPS data of -System, instead of the GPS data of the IP device.

11.15.4 Viewing GPS Locations during Playback

To play back the recorded GPS locations with videos, follow the steps below.

1. On the ViewLog window, click the **Tools** button and click **Select Map API** to select a map API (Application Program Interface). This dialog box appears.

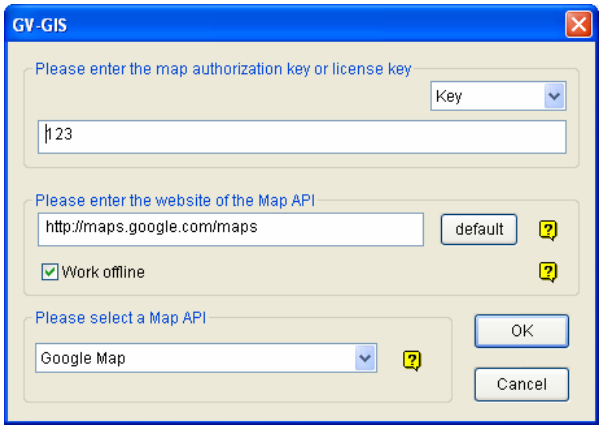


Figure 11-90

2. Under **Please Select a Map API**, select a Map API.
3. To play back GPS data, click the **Tools** button and select **Display GIS Window**. The first-time user will be prompted for a License Agreement. Read through the license terms before you click **I understand and agree** to continue.
4. Select the events with GPS data from the Video Event list, select the desired video mode, and click the **Play** button to start.

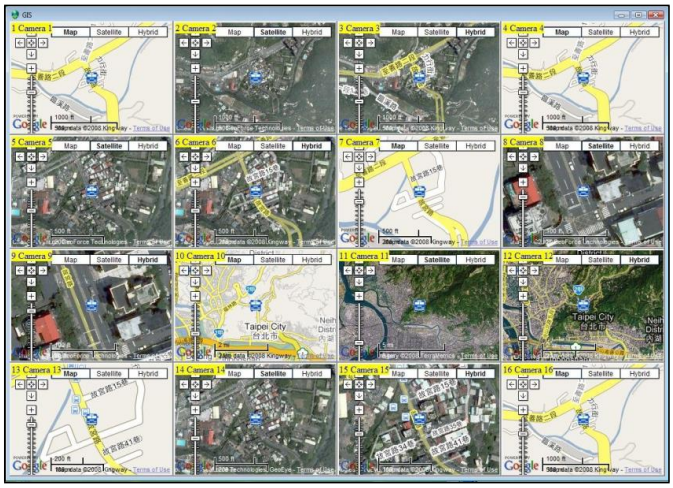


Figure 11-91

Note:

1. If you like to use the maps created yourself, overwrite the files at :\ folder\GIShtm-User, and select **User Defined** from the “Please Select a Map API” drop-down list (Figure 11-90).
2. If you are the paid-client of Google Maps, select **Client** from the “Please enter the map authorization key or license key” drop-down list; otherwise select **Key.**

11.15.5 Sending GPS Data to the -GIS

You can configure up to 4 -GIS stations to receive the GPS data of the -System and connected IP devices simultaneously.

Sending Only GPS Data of the -System

To send only GPS data of -System to the -GIS station, follow the steps below. On the -GIS station, a **Mobile Host** account for -System needs to be created first.

1. To allow the remote access from -GIS to -System, enable **Control Center Server** from the **Network** button on the main screen.
2. Click the button on the -GIS Client window (Figure 11-87). This dialog box appears.

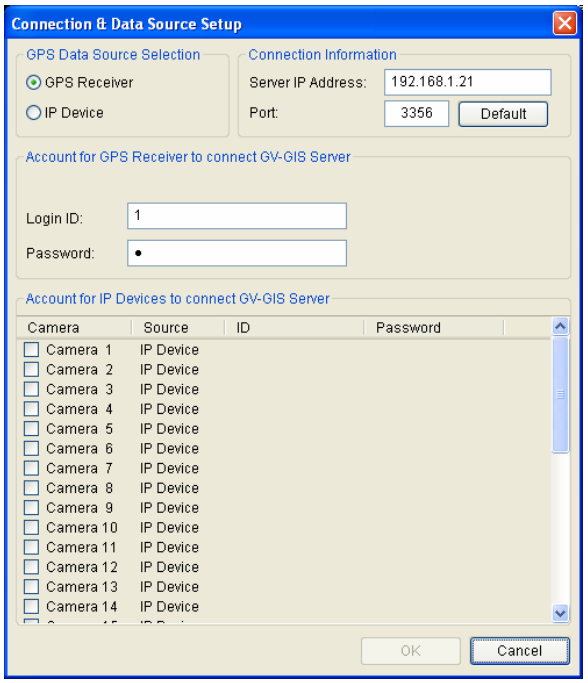


Figure 11-92

3. In the GPS Data Source Selection section, select **GPS Receiver**.
4. In the Connection Information section, type the IP address of -GIS. Keep the default port value of 3356, or modify it if necessary.
5. In the Account for GPS Receiver to Connect -GIS Server section, type login ID and password already created on -GIS for -System.
6. Click **OK**.

7. To create connection to other -GIS stations, double-click # 2 to # 4 columns on the -GIS Client window and configure the connection information by following above steps.
8. To start connecting to -GIS, click the button. The GPS data of -System will be sent to -GIS.

Sending GPS Data of both -System and Connected IP Devices

You can not only send the GPS data of -System to the -GIS station, but also those of connected IP devices. On the -GIS station, the **Mobile Host** accounts for -System and IP devices need to be created individually in advance.

1. To allow the remote access from -GIS to -System, enable **Control Center Server** from the **Network** button on the main screen.
2. Ensure **Enable GIS Data** is enabled for desired IP devices to receive the GPS data from those IP devices (Figure 11-89).
3. Click the button on the -GIS Client window (Figure 11-87). This dialog box appears.

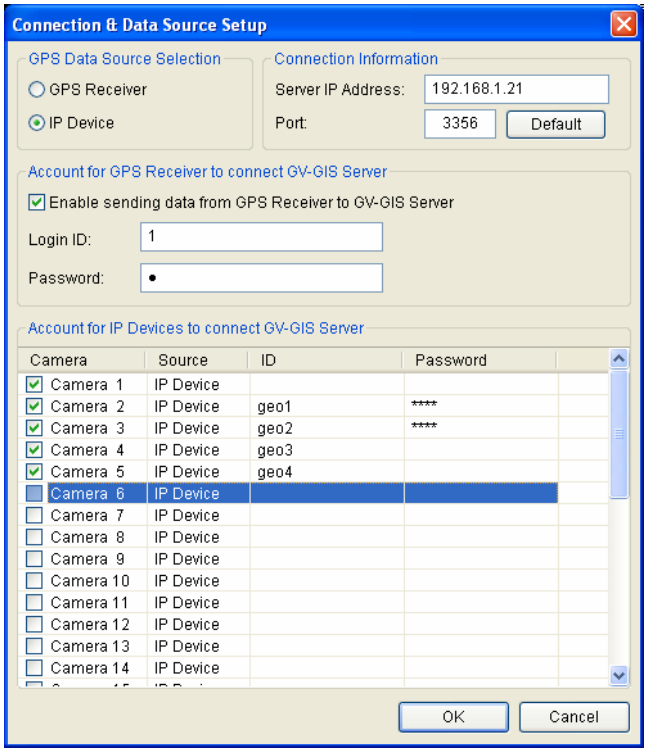

Connection & Data Source Setup
GPS Data Source Selection
GPS Receiver
IP Device
Connection Information
Server IP Address: 192.168.1.21
Port: 3356
Default
Account for GPS Receiver to connect GV-GIS Server
Enable sending data from GPS Receiver to GV-GIS Server
Login ID: 1
Password:
Account for IP Devices to connect GV-GIS Server
Camera Source ID Password
Camera 1 IP Device
Camera 2 IP Device geo1 ****
Camera 3 IP Device geo2 ****
Camera 4 IP Device geo3
Camera 5 IP Device geo4
Camera 6 IP Device
Camera 7 IP Device
Camera 8 IP Device
Camera 9 IP Device
Camera 10 IP Device
Camera 11 IP Device
Camera 12 IP Device
Camera 13 IP Device
Camera 14 IP Device
OK
Cancel

Figure 11-93

4. In the GPS Data Source Selection section, select **IP Device**.
5. In the Connection Information section, type the IP address of -GIS. Keep the default port value of 3356, or modify it if necessary.

6. In the Account for GPS Receiver to connect -GIS Server section, type login ID and password created on -GIS for the -System.
7. In the Account for IP Device to connect -GIS Server section, select desired IP cameras and type their separate login IDs and passwords created on -GIS.
8. Click **OK**. The **Connection(s)** column on the -GIS Client window will display the total number of to-be-connected devices which includes one -System and the number of connected IP cameras.
9. To create connection to other -GIS stations, double-click # 2 to # 4 columns on the -GIS Client window and configure the connection information by following above steps.
10. To start connecting to -GIS, click the button. The GPS data of -System and connected IP devices will be sent to -GIS.

11.16 -IP Device Utility

The IP Device utility can detect -IP devices in the LAN and allows you to quickly set the IP address of the device, upgrade firmware, export/import device settings and reboot the device. In addition, with the Utility, you can map IP cameras to the channels of -System, and export and import the camera mapping settings.

11.16.1 Installing -IP Device Utility

1. Insert the Software DVD to your computer. It runs automatically, and a window appears.
2. Click **Install Sting Alarm Supplemental Utilities**.
3. Select **-IP Device Utility**, and follow the on-screen instructions.

11.16.2 The -IP Device Utility Window

To start the -IP Device Utility, go to Windows **Start**, point to **Programs**, select **IP Device Utility**, and then run **IP Device Utility**. The window below appears and automatically searches for any -IP device under LAN.

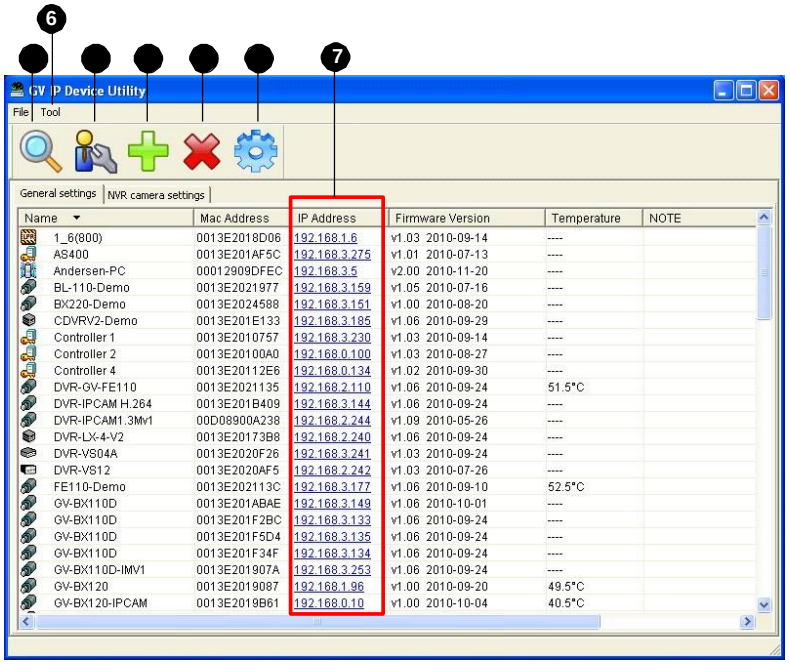


Figure 11-94

The controls in the window:

No.	Name	Description
1	Search	Searches for available -IP devices under LAN.
2	Auto Set IP Address	Automatically assigns unused IP addresses on the LAN to the IP addresses with the same ID and Password.
3	Add	Adds an IP device to the list or import an excel file to add multiple IP devices. A template of the excel file is located in the folder where -IP Device Utility is installed.
4	Delete	Deletes the IP device from the list.
5	Configure	Specifies the network adaptor.
6	Tool (on the menu bar)	④ **Configure:** Specifies the network adaptor. ④ **Temperature Monitor:** Select the temperature unit and specify the temperature
7	IP Address	Directs to the Web interface of the IP address.

11.16.3 Setting IP Devices

1. Double-click the -IP device to open the setting page of the device.

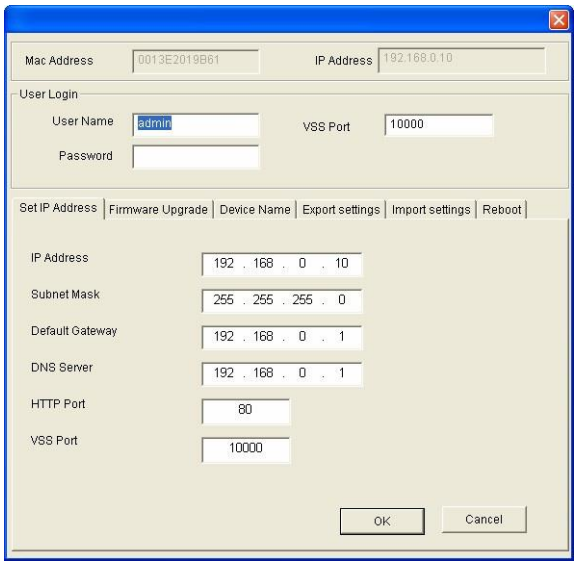


Figure 11-95

2. Click the different tabs to access the following settings:

[Set IP Address] Type the IP address, subnet mask, default gateway and DNS server of the device. You can also customize the HTTP port and VSS port.

[Firmware Upgrade] To upgrade the firmware of the device, click **Browse** to specify the path of the firmware file and click **Upgrade** to proceed. You can select **Upgrade all devices** to upgrade all other IP devices of the same username, password and model.

[Device Name] Type a name for the device.

[Export settings] Click **Browse** to specify a path. Click the **Export Settings** button to export the device settings.

[Import Settings] Specify the location of the file to import camera settings to an IP device. If **Upgrade all devices** is selected, the settings will apply to all other devices of the same username, password and model. You can select **Password settings** and **Network settings** to also import the password and network settings.

[Reboot] Click **Reboot** to reboot the device or click **Light Show** to make the device LED flash.

11.16.4 Mapping IP Cameras

You can map IP cameras to the channels of -System by using the IP Device Utility. Click the **NVR Camera Settings** tab on the IP Device Utility window and the following window appears:

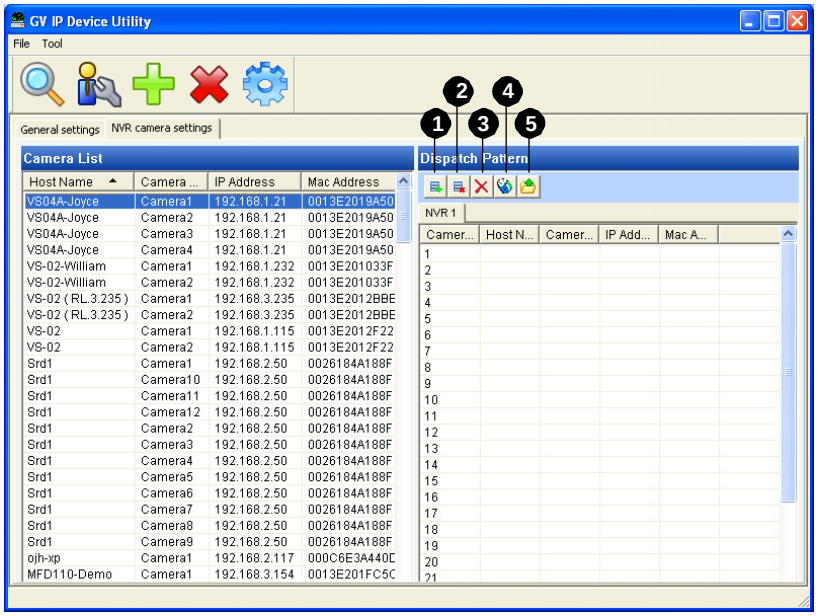


Figure 11-96

The buttons in the Dispatch Panel toolbar:

No.	Name	Description
1	Add	Adds a new tab to create another set of IP camera settings.
2	Delete	Deletes the selected tab.
3	Delete Selection	Deletes the selected IP camera from the Dispatch Pattern section.
4	Clear All	Clears all IP cameras in the selected tab.
5	Export	Exports the IP camera mapping settings.

To map IP cameras to the channels of -System:

1. Drag one or multiple IP devices from the **Camera List** to the desired camera channels in the **Dispatch Pattern** section.
2. By default, the login username and password for the IP camera both are set to **admin**. If the added IP camera does not use the default settings, you need to right-click the IP camera in the **Dispatch Pattern** section and select **Login User Information** to modify its logon information.
3. You can use the Export button to export the IP camera mapping settings and then import the settings back into the Main System. See *Camera Mapping Using IP Device Utility* in Chapter 2.

11.17 MCamCtrl Utility for -Joystick

The MCamCtrl Utility is an independent application that allows you to control -PTZ Camera, -PT Camera, -IP Speed Dome, and any PTZ camera connected to -Video Server and -Compact DVR using a -Joystick.

You just need to run the MCamCtrl Utility on the computer connected with a -Joystick, and open the Web interface of the specific IP device. You can remotely control the PTZ movement using the -Joystick.

11.17.1 Installing MCamCtrl Utility

To install the MCamCtrl Utility on the computer connected with a -Joystick:

1. Insert the Software DVD to your computer. It runs automatically, and a window appears.
2. Click **Install Sting Alarm Supplemental Utilities**.
3. Select **-MCamCtrl Utility**, and follow the on-screen instructions.

11.17.2 Starting the MCamCtrl Utility

1. Go to Windows **Start**, point to **Programs**, select **MCamCtrl**, and then run **MCamCtrl**. The MCamCtrl dialog box appears.

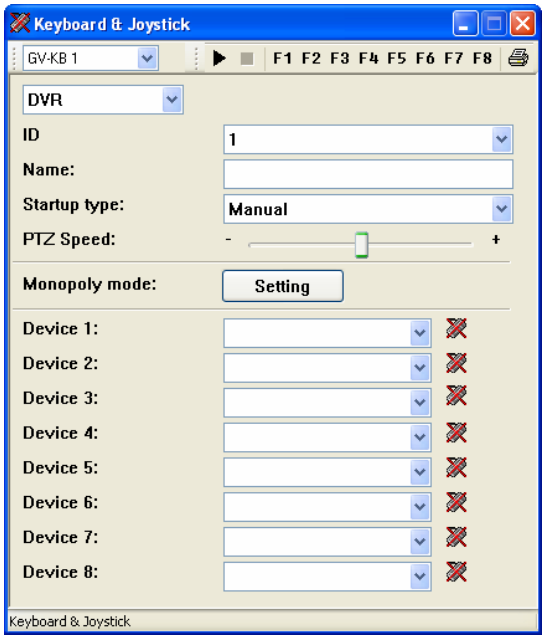


Figure 11-97

2. Leave both ID and Name fields blank.
3. In the Startup Type field, select **Manual** or **Automatic** to run MCamCtrl at next startup.
4. To adjust the PTZ speed, use the slide bar.
5. In the Device field, select the port connecting to the -Joystick. To find out the port number the -Joystick is using, go to **Windows Device Manager** and look for the Prolific USB to Serial Bridge entry under the Ports (COM & LPT) section.
6. Click the **Start Service** button ► to start the service.
7. Keep the MCamCtrl Utility running in the background, and open the Web interface of the IP device to begin controlling the PTZ movement using -Joystick.

11.18 -Mobile Server

-Mobile Server is an application that can encode up to 32 video channels and allows live view access from -IP Decoder Box, -Pad and mobile devices including Android Smartphone, iPad, iPhone and iPod Touch. Third-party surveillance software can also access video channels from -Mobile Server through RTSP.

For more details, refer to the -*Mobile Server User Manual* on the Software DVD.

11.19 Language Setting

11.19.1 MultiLang Tool for Translated Text

The user interface has been translated from English into 30 other languages. If you find the translation to be unsuitable and would like to correct it, you can use the MultiLang Tool to revise the translation. Next, you can apply the revised text to the applications and export a MRevise.exe file to make the same revision on another computer. You can also send the revision back to Sting Alarm to have the revision included in future software releases.

Note: When using the MultiLang Tool, it is recommended to revise an entire sentence at a time instead of simply searching a single word and replacing the word in all other strings.

To revise the translated text:

1. Insert the Software DVD to your computer. It runs automatically, and a window appears.
2. Click **Install Sting Alarm Supplemental Utilities**.
3. Select **-MultiLang Tool** and follow the on-screen instructions.
4. Close all Sting Alarm applications first and then double-click **MultilingualConfig.exe**. This dialog box appears.

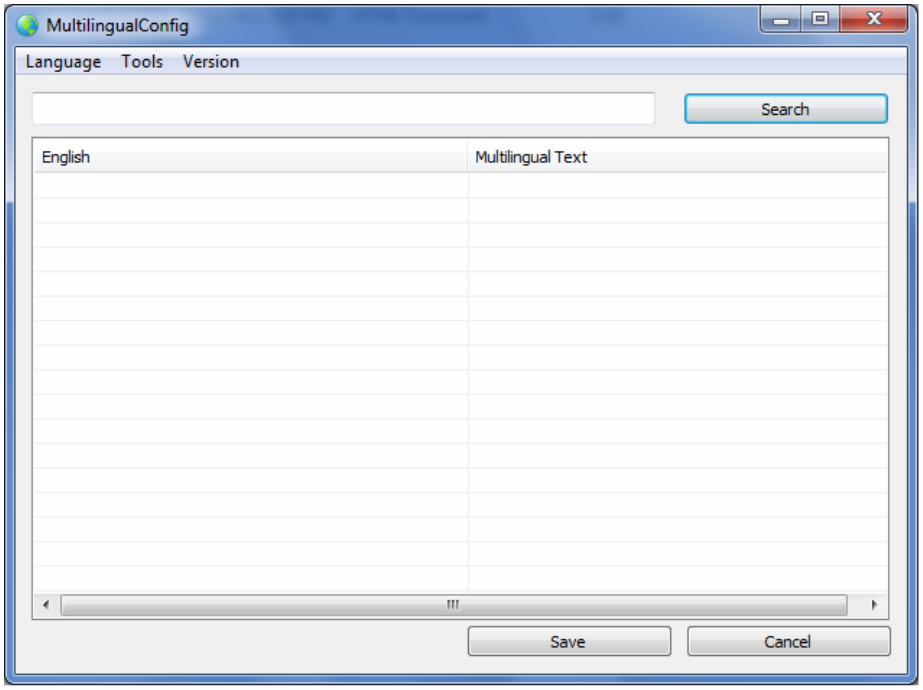


Figure 11-98

5. Click **Language** and select the language of the text you want to revise.
6. Click **Version** to select the version of the Main System that you want to revise.

7. In the **Search** field, type all or part of the text in English or the target language and click **Search**.

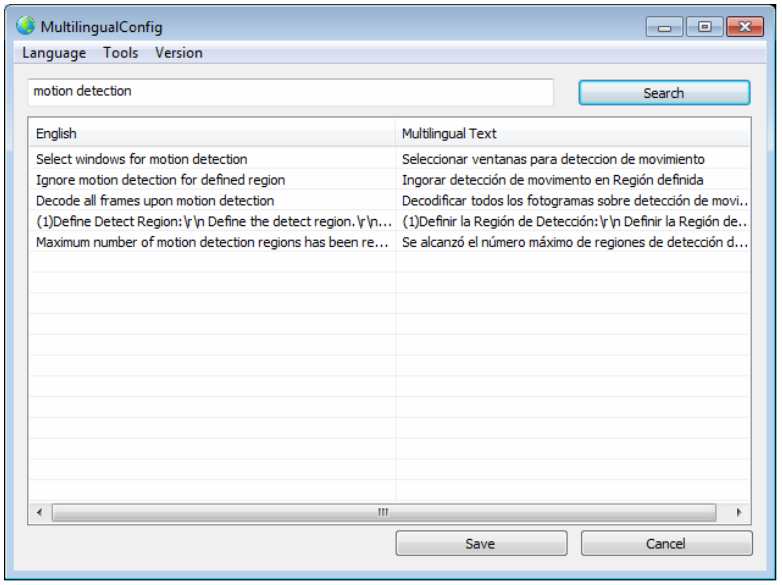

MultilingualConfig
Language Tools Version
motion detection
Search
English
Multilingual Text
Select windows for motion detection
Seleccionar ventanas para deteccion de movimiento
Ignore motion detection for defined region
Ingorar detección de movimento en Región definida
Decode all frames upon motion detection
Decodificar todos los fotogramas sobre detección de movi..
(1)Define Detect Region:\r\n Define the detect region.\r\n...
(1)Definir la Región de Detección:\r\n Definir la Región de..
Maximum number of motion detection regions has been re...
Se alcanzó el número máximo de regiones de detección d...
Save
Cancel

Figure 11-99

Note:

1. The search is case sensitive.
2. Before making any revision, click **Tools** and select **Revision Note** to read the revision instructions.

---

8. Double-click the text you want to revise. This dialog box appears.

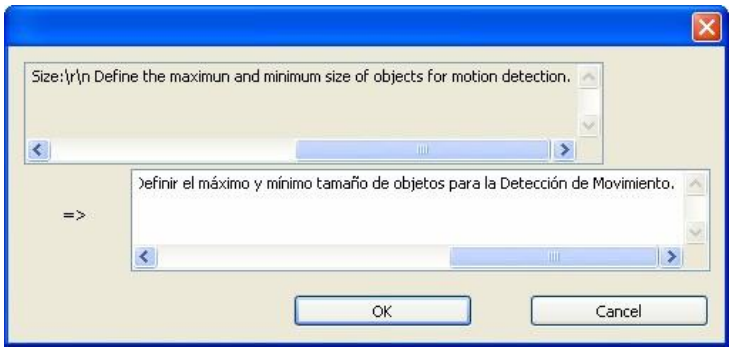

Size:\r\n Define the maximun and minimum size of objects for motion detection.
=>
)efinir el máximo y mínimo tamaño de objetos para la Detección de Movimiento.
OK
Cancel

Figure 11-100

9. Revise the translated text and click **OK**.

Tip: The text may contain symbols such as **%d** or **\n** that instruct the application to perform certain functions. Be careful not to change the symbols in the translated text.

To apply the revised text:

1. To apply the revised translation to the applications, click **Save**. For the following applications, the system will automatically locate the corresponding files on your computer and replace with the revised translation.
    - -System
    - Remote ViewLog
    - Fast Backup and Restore (FBR)
    - -IP Device Utility
    - Multi View
    - Remote E-Map
    - Center V2
    - Vital Sign Monitor
    - Dispatch Server
    - -GIS
    - MCamCtrl Utility
    - POS Text Sender
    - Authentication Server
    - SMS Server
    - Audio Broadcast
    - Multicast
    - TwinDVR System
    - Bandwidth Control Client Site
    - Backup Viewer
    - Mobile Server

2. After applying the revision, a dialog box appears to show which applications have been revised. Click **OK**.

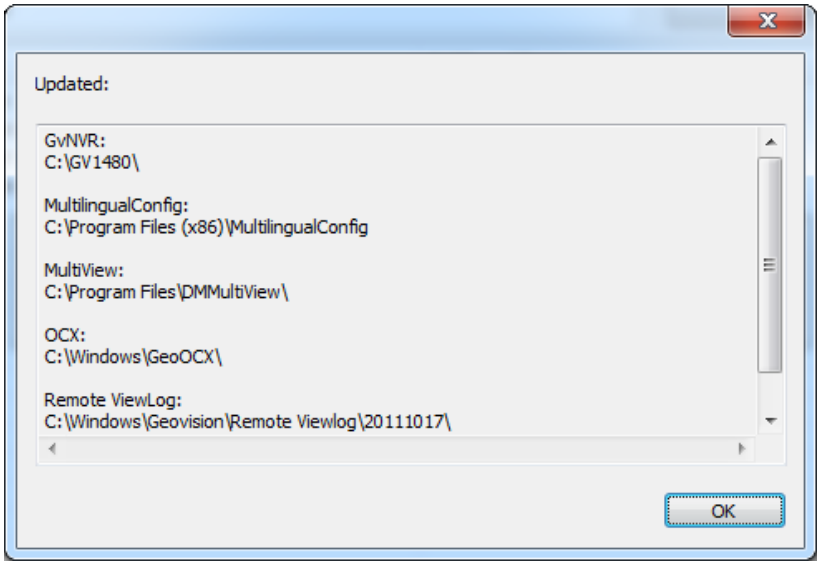


Figure 11-101

3. The message "*Do you want to apply the revised multilingual texts to another folder?*" appears. If the storage path for the application has been changed or if the associated application is not listed in the dialog box, click **Yes** and select the folder of the application.

To export or send the revised text:

1. To export the revision as an executable file, click **Tools**, **Export** and **Export executable file**. You can copy the .exe file to another computer and apply the same translation revision by running the .exe file.
2. To report the translation revision back to Sting Alarm,
   - If your default mail client is Outlook, Outlook Express or Mozilla Thunderbird, click **Tools**, **Export** and **Send Report** to send the revision.
   - If your default mail client is not set up or supported, click **Tools**, **Export** and **Export text file**, and email the exported text file to localize@Sting Alarm.com.tw.
3. For the distributors to duplicate Software DVD with the translation revision,
   - Copy and paste all the contents of Software DVD to your computer.
   - Export the revised translation file and rename the file as **MRevise.exe**.
   - Move **MRevise.exe** to the location you saved the contents of Software DVD **:\Software\Translation Revision.**
   - Duplicate the Software DVD with the **MRevise.exe** file.
   - Test the Software DVD by clicking **10. Import Translation Revision** from the Install Program window to apply the translation revision.

11.19.2 SetLanguage Tool to Set UI Language

The default user interface (UI) language of the following -software and applications is set according to the region detected. You can install the Set Language tool to set the UI language to English.

- -System
- -Fast Backup and Restore Multicam System
- ViewLog / EZViewLog
- -Remote ViewLog
- -POS Text Sender
- -IP Device Utility
- -Center V2
- -Vital Sign Monitor
- -Dispatch Server
- -Control Center
- -Remote E-Map
- CMS Lite.

To install the Set Language tool:

1. Insert the Software DVD to your computer. It runs automatically, and a window appears.
2. Click **Install Sting Alarm Supplemental Utilities**, select **-SetLanguage** and follow the on-screen instructions.
3. After completing the installation, close all Sting Alarm software or applications.
4. At the **Start** menu, Select **SetLanguage**.
5. When the **Configure** window appears, use the **Language** drop-down list to select **English**.

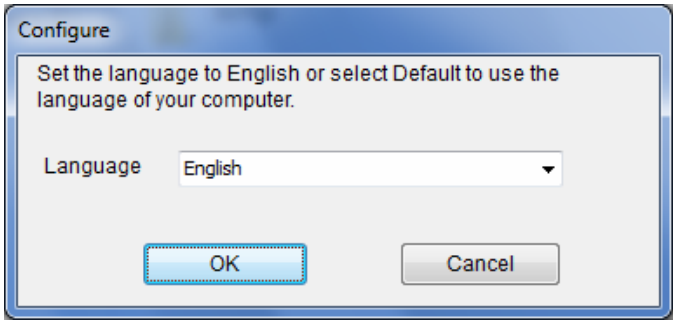


Figure 11-102

6. Click **OK** and restart your -software or application to enable English UI.

11.20 Skype Video Utility

The Sting Alarm Skype Video Utility allows you to receive live view or text notifications through a Skype account using a PC or mobile device upon motion detection or input trigger. You will need to install Skype on the computer of the -System, and the notifications can be sent to other Skype accounts.

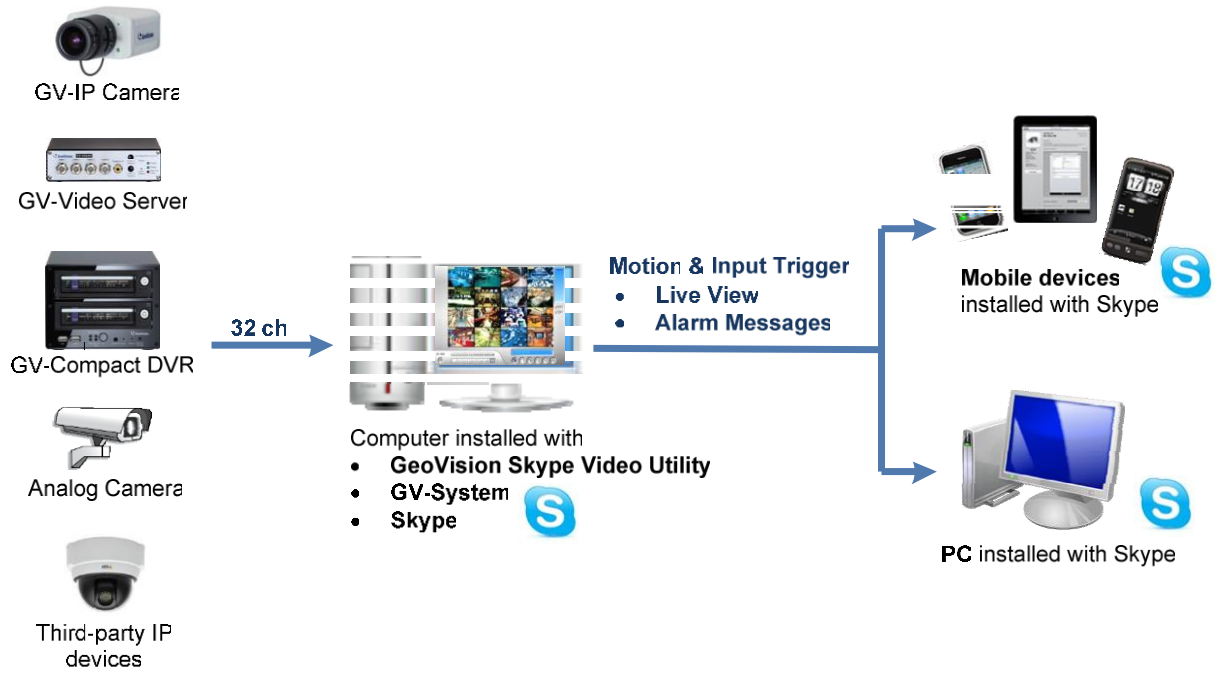


Figure 11-103

Note: Audio function is not supported in -Skype Video Utility.

11.20.1 Installing -Skype Video Utility

1. Insert the Software DVD to your computer. It runs automatically, and a window appears.
2. Click **Install Sting Alarm Supplemental Utilities**.
3. Select **-Skype Video Utility**, and follow the on-screen instructions.

Note: Before running the utility, make sure you have logged in your Skype account and -System.

4. Double-click the **-Skype Video Utility.exe** icon on the desktop. The utility begins to connect to Skype.
5. A dialog box appears on your Skype. Click **Allow access**.

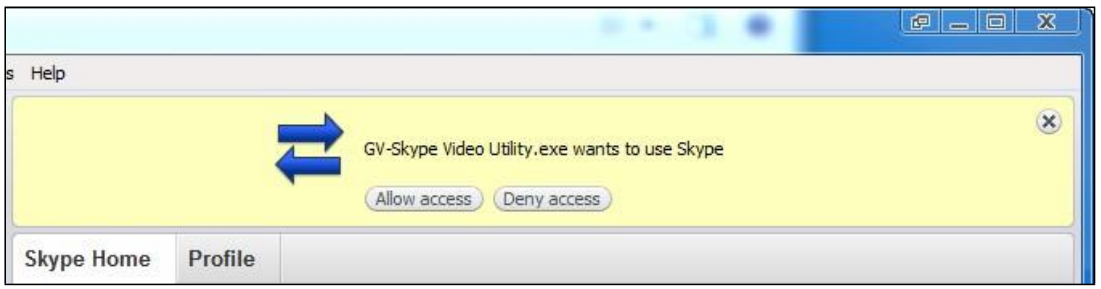


Figure 11-104

After connected to Skype successfully, the -Skype Video Utility will minimize to system tray.

11.20.2 Setting Up Notifications Upon Motion or I/O Trigger

General Setting

1. Right-click the **-Skype Video Utility** icon

in the system tray and click Settings. This dialog box appears.

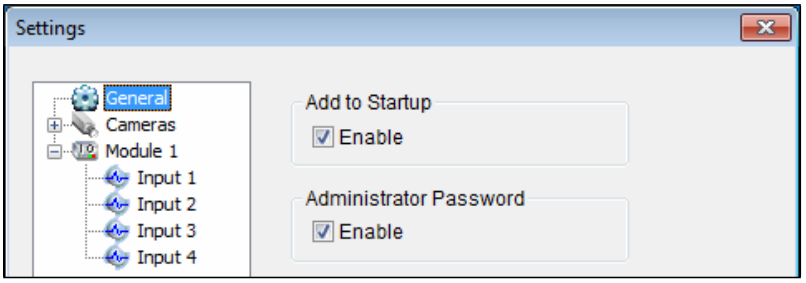


Figure 11-105

2. The General setting page offers the following options:

   ④ **Add to Startup:** Click **Enable** to automatically run -Skype Video Utility at Windows startup.

   ④ **Administrator Password:** Click **Enable** to require password to log in and out of -Skype Video Utility.

Camera Setting

To send camera live view or notification message to Skype accounts upon motion detection, expand the Cameras list and select a camera. This dialog box appears.

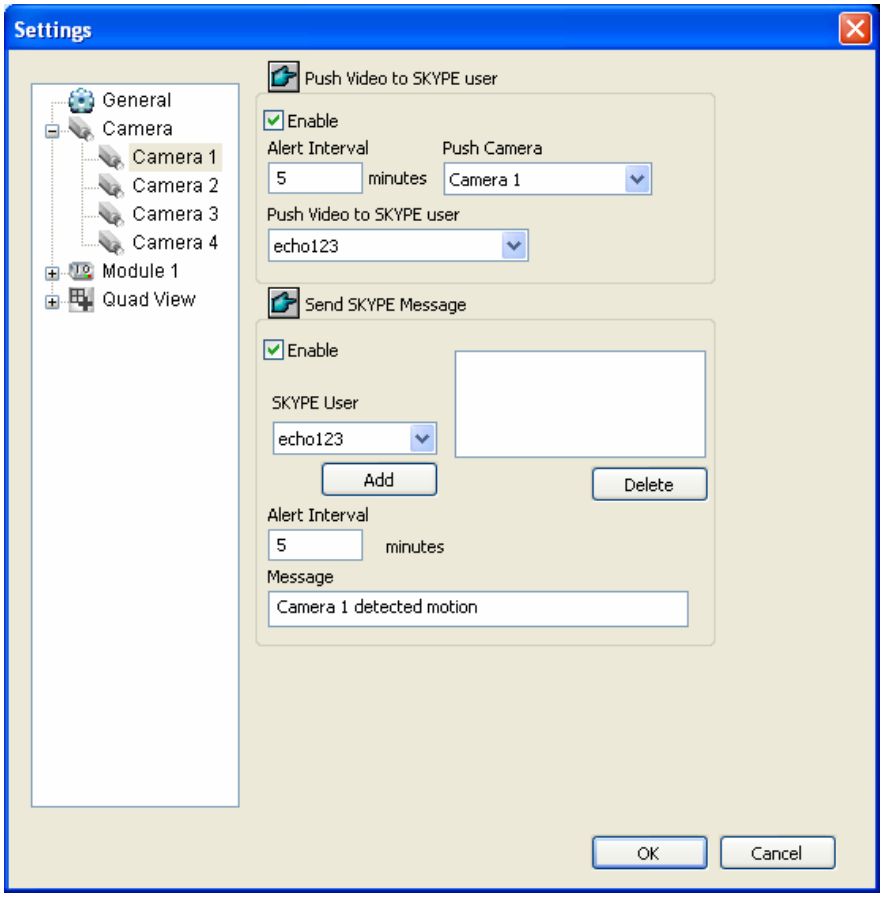


Figure 11-106

To Send the Live View

You can send live view from the selected camera or quad view to a Skype account upon motion.

1. Select **Enable** under Push Video to Skype User.
2. Set an **Alert Interval** to specify the minimum time between each notification.
3. Select a desired camera or a quad view from the **Push Camera** drop-down list. (See *To Create a Quad View* in this chapter later.)
4. Use the **Push Video to SKYPE user** drop-down list to select a Skype user to send live view.

Note:

1. -Skype Video Utility can only send camera live view to one Skype account at a time.
2. The received camera live view will be displayed in Skype's default resolution.

To Create the Quad View

1. Click **Quad View** and select a quad view. This dialog box appears.

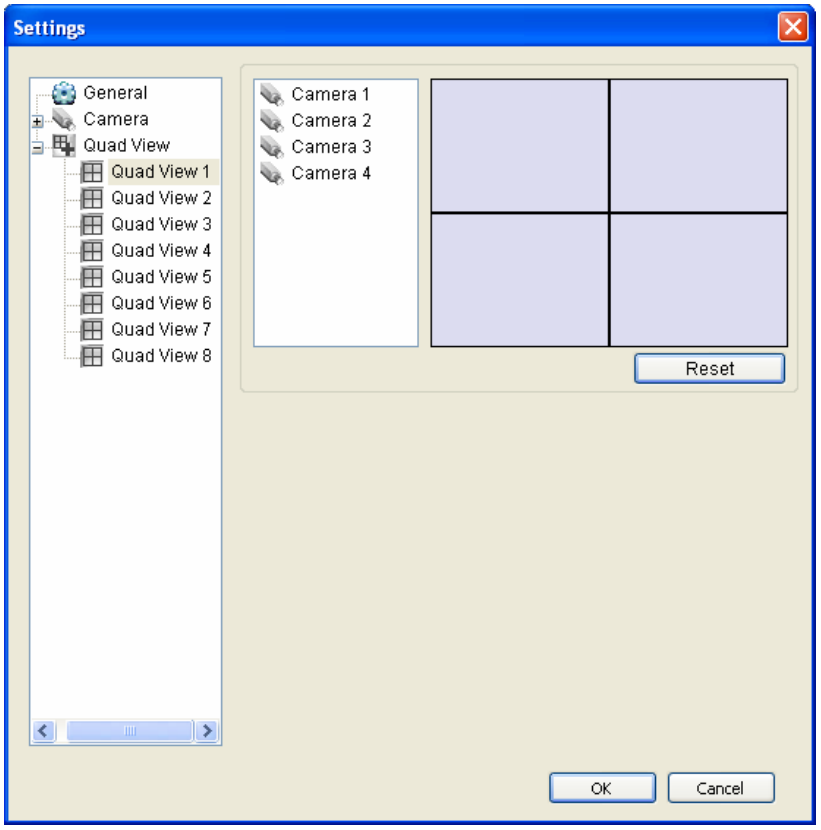


Figure 11-107

2. Drag and drop up to four cameras to the quad view on the right.
3. Click **OK**.

To Send a Notification Message

You can send notifications to multiple Skype accounts upon motion.

1. Select **Enabl**e under Send Skype Message.
2. Use the **Skype User** drop-down list to select the recipient of the message and click the **Add** button. Repeat for any additional recipient.

3. Set an **Alert Interval** to specify the minimum time between each notification.
4. Type a notification message up to 255 characters.

Input Module Setting

To send camera live view or notification message to Skype accounts upon input trigger, expand the **Module** list and select an input device. This dialog box appears.

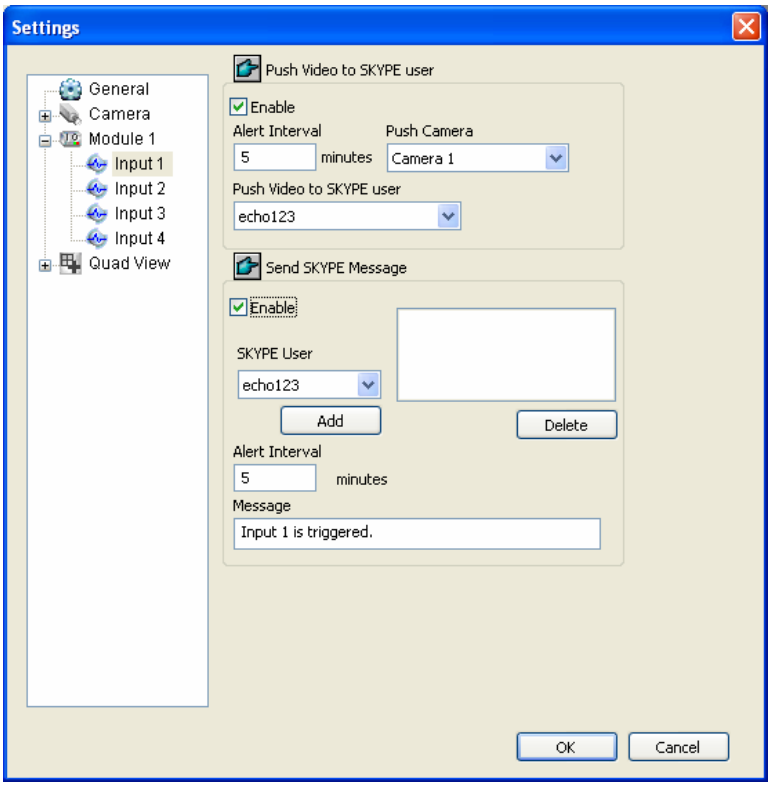


Figure 11-108

1. To send live view to a Skype account of a camera upon input trigger, follow the steps from *To Send the Live View* in the previous *Camera Setting* section.
2. To send a notification message to multiple Skype accounts upon input trigger, follow the steps from *To Send a Notification Messages* in the previous *Camera Setting* section.
3. Click **OK** to apply the setting.

Receiving Notification Messages and Live View

After setup is completed, the designated Skype user will see a notification message, as well as an incoming call to receive live view upon motion detection or input trigger.

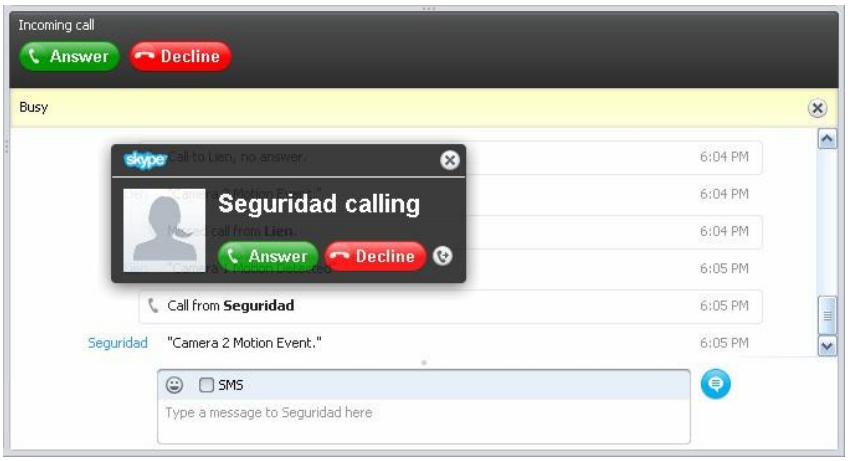


Figure 11-109

Click the **Answer** button to receive camera live view. When you finish watching the live view, click the red phone button to end the video call.

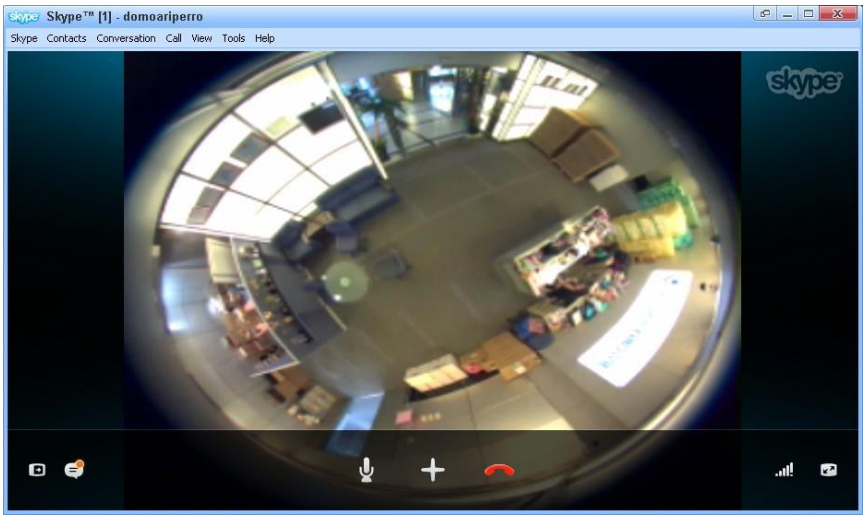


Figure 11-110

Note: If the incoming call is not picked up, the Skype user will see a missed call record in the call history.

Requesting Live View from a Remote PC or Mobile Device

1. Log in Skype and select the Skype account of the -Skype Video Utility from Contact.
2. Click the **IM** button and type **Cam 1** to view the channel 1 or type other channel numbers. To view single channel live view, type channels 1 to 32. To view one of the 8 quad views, use channels 33 to 40.

Figure 11-111

3. Click **Send** and an incoming call will appear momentarily.

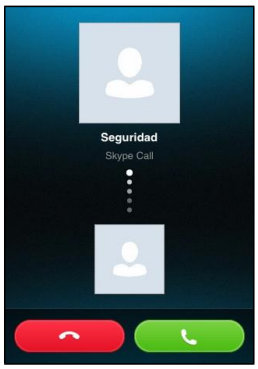


Figure 11-112

4. Click the green **Answer** button to watch the live view.

Figure 11-113

Note: You can back up the settings on the utility by using Fast Backup and Restore. See *Fast Backup and Restore* earlier in this chapter.

Appendix 629

A. USB Dongle Required for IP Device Applications 629
B. Supported PTZ Protocols and Models 630
C. Certified PTZ Models for Object Tracking 632
D. Certificated PTZ Models for Full Degree Pan and Tilt Control 633
E. Supported IP Device Brands 634
F. Supported GPRS Models 635
G. Custom Icon Naming Chart for Multi View 636
H. Display Ratio Supported by Panel Resolution 637
I. Dual Stream Support List 638

Appendix

A. USB Dongle Required for IP Device Applications

Solution	Application	USB Dongle
-Hybrid DVR	Connection of 3rd party IP devices to -System	**NVR** Dongle
-NVR	Connection of 3rd party IP devices to -NVR	**NVR** Dongle
-Center V2	Connection of IP devices to Center V2	No extra dongle required
Note: Currently, -Center V2 does not support the connection with 3rd party IP devices.		

B. Supported PTZ Protocols and Models

Note that -System only supports original factory models. Other brands of cameras claiming of the same protocol compatibility may not work properly with -System. Sting Alarm takes no responsibility of such incompatibility.

PTZ Model and Protocol
AcutVista (SSD-7971D)
Ademco (Jupiter)
Bosch (G3)
Bosch (TC700 / 8560)
Canon (VCC4 / VCC5i)
CBC GANZ (ZC-S120 Series)
Chiper (CPT-V9KRV)
COP (15-CD53W) - Pelco D
COP (15-CD55TW) - Pelco D
COP (15-CD55W) - Pelco D
COP (CD55X) - Pelco D
Direct Perception (PTU Series)
D-max Dome
DongYang Dome (DOH-240)
DynaColor (D-7720 / 7722)
DynaColor Dome
Dynacolor (DynaHawk-ZH701)
ELBEX (Matrix / 1000)
Elmo (PTC-200C)
Elmo (PTC-400C)
Elmo (PTC-1000)
EverFocus (EPTZ 1000 / 500)
Eyeview T-Power (T2-SA27)
GKB (SPD-221)
HiSharp - Pelco D
HiSharp - Pelco P
JEC Dome
JVC (TK-S576B / S655 / C686E)
Kalatel CyberDome
Kampro Technology (K-ZC23)

KenKo (DMP23-H1)
LG (LPT-OS553HQ)
Lilin (PIH) – MLP1
Lilin (PIH-7625) – MLP1
Lilin (PIH-820) – MLP1
MESSOA (SDS600 Series)
MESSOA (D-700 Series)
Minking Dome
Mintron (54G2AHN / P)
NanWang (NVD 2300PNT)
NanWang V4.1 (NVD 2300PNT)
Panasonic (WV-CS850)
Panasonic (WV-CW960)
Pelco Dome
Pelco (Spectra III)
Pelco Spetra Mini Dome (SD4-WO)
Pishion (22X)
PTZ in I/O
RX214D
SAE (DR-E588)
Samsung (SCC-641 / 643)
Samsung (SPD-1600)
Samsung (SPD-3300)
Sensormatic (Ultra IV)
Sony (EVI-D100)
StorVision PTZ
TOA (CC551)
VDI (CT-58SPD)
VIDO.AT Dome
YAAN Dome
360 Vision (ViD-18COP04) - Pelco P

C. Certified PTZ Models for Object Tracking

The PTZ models listed below are tested and certified by Sting Alarm for their compatibility with the Object Tracking function.

Dual-Camera Tracking (Object Tracking and Zooming)

Brand / Model
AcutVista (SSD-7971D)
Dynacolor (DynaHawk Zh701)
Sting Alarm (-SD010 Series, -SD220 Series)
Messoa (SDS600 Series)
Messoa (D-700 Series)
Pelco (Spectra III)
Sensormatic (Ultra IV)
VIDO. AT Dome

Advanced Single Camera Tracking

Brand / Model
AcutVista (SSD-7971D)
COP (15-CD55W) - Pelco D
Sting Alarm (-SD010 Series, -SD200 Series , -SD220 Series)
Lilin (PIH-7625) – MLP1
Messoa (D-700 Series)
Pelco (Spectra III)
VIDO.AT Dome

D. Certificated PTZ Models for Full Degree Pan and Tilt Control

Brand / Model	Slope and Random Modes Support	Random Mode Support Only
AcutVista (SSD-7971D)	√	
Bosch (G3)		√
COP (15-CD53W) - Pelco D	√	
COP (15-CD55TW) - Pelco D	√	
COP (15-CD55W) - Pelco D	√	
COP (CD55X) - Pelco D		√
Dynacolor (Dynahawk-Zh701)	√	
Dynacolor Dome		√
D-max Dome		√
Sting Alarm (-IP Speed Dome)	√	
JVC (S655 / TK-C686E / TK-S576B)	√	
Lilin (PIH-7625) – MLP1	√	
Lilin PIH – MLP1	√	
Lilin (PIH-820) – MLP1		√
Messoa (SDS600 Series)		√
Messoa (D-700 Series)	√	
Pelco D	√	
Pelco P	√	
Pelco Spetra Mini Dome (SD4-W0)		√
Pelco (Spectra III)	√	
Samsung (SCC-641 / SCC-643)	√	
StorVision		√
VDI (CT-58SPD)	√	
VIDO AT Dome	√	

E. Supported IP Device Brands and Protocols

This list provides the supported IP device brands. For detailed information on the supported IP devices, refer to Supported IP Camera List on Sting Alarm's Website: http://www.Sting_Alarm.com.tw/english/4_21.asp

IP Devices
Sting Alarm
ACTi
Arecont Vision
AXIS
Bosch
Canon
CNB
D-Link
Etrovision
Hikvision
HUNT
IQinVision
JVC
LG
Messoa
MOBOTIX
Panasonic
Pelco
Samsung
Sanyo
SONY
UDP
Verint
VIVOTEK
Protocols
ONVIF
PSIA
RTSP

F. Supported GPRS Models

Brand	Model
Round Solutions	TER-GX series
Wavecom	Multiband 900E 1800 GSM Modem

G. Custom Icon Naming Chart for Multi View

This chart lists all the default icons with their filenames as a reference for users who wish to replace icons on the Multi View window. To replace an icon on the Multi View window, simply rename your custom icon name to one of relevant icon name listed below.

DVR	Size	Icon		Default Host	Size	Icon
dvr16.bmp	16x16			addrbook_defaulthost.bmp	22x22	
dvr24.bmp	24x24					
addrbook_dvr16.bmp	16x16			Authentication Host	Size	Icon
addrbook_dvr22.bmp	22x22			addrbook_authsvrgrouop.bmp	22x22	
-Video Server	Size	Icon		Multiple Host	Size	Icon
VS16.bmp	16x16			addrbook_host16.bmp	16x16	
VS24.bmp	24x24			addrbook_host22.bmp	22x22	
addrbook_vs16.bmp	16x16					
addrbook_vs22.bmp	22x22			Group	Size	Icon
				addrbook_group16.bmp	16x16	
-IPCAM	Size	Icon		addrbook_group22.bmp	22x22	
ipcam16.bmp	16x16					
ipcam24.bmp	24x24			Camera	Size	Icon
addrbook_ipcam16.bmp	16x16			addrbook_camera.bmp	22x22	
addrbook_ipcam22.bmp	22x22					
				Off-host	Size	Icon
-Compact DVR	Size	Icon		addrbook_webcamoffhost.bmp	22x22	
compactdvr16.bmp	16x16					
compactdvr24.bmp	24x24					
addrbook_compactdvr16.bmp	16x16					
addrbook_compactdvr22.bmp	22x22					
-Video Gateway	Size	Icon				
videogateway16.bmp	16x16					
videogateway24.bmp	24x24					
addrbook_videogateway16.bmp	16x16					
addrbook_videogateway22.bmp	22x22					

H. Display Ratio Supported by Panel Resolution

The display ratio supported by each types of panel resolution is listed below:

Panel Resolution	Supported Display Ratio
800 x 600	4:3
1024 x 768	4:3
1280 x 1024	5:4
1680 x 1050	16:10
1600 x 1200	4:3
1920 x 1200	16:10
1280 x 800	16:10
1920 x 1080	16:9
1440 x 900	16:10

I. Dual Stream Support List

The table lists the firmware versions of -IP devices that support dual stream and the default resolutions after the camera is added to -System.

-IP Camera	Supported Firmware Version	Resolution	
		Main Stream (H.264)	Sub Stream (MJPEG)
-BX120D	V1.00 or later	1280 x 1024	320 x 256
-BX1200 Series	V1.15 or later		
-MFD120	V1.05 or later		
-BX120D-E -CBW120 -MDR120	V1.07 or later		
-BL120D -VD120D -VD121D -VD122D -VD123D	V1.02 or later		
-FD120D -CB120	V1.03 or later		
-UBX1301 Series	V2.04 or later		
-UBL1211 -UBL1301 Series	V2.05 or later		
-BX130D Series -MFD130 -BL130D	V1.04 or later		
-BX1300 Series -CA120 -CAW120	V1.15 or later		
-BX140DW	V1.10 or later	1280 x 720	640 x 360
-BX220D Series	V1.00 or later	1920 x 1080	448 x 252
-BX2400 Series	V1.15 or later		
-MFD220	V1.05 or later		
-BX220D-E -CBW220 -MDR220	V1.07 or later		

-IP Camera	Supported Firmware Version	Resolution	
		Main Stream (H.264)	Sub Stream (MJPEG)
-BL220D - VD220D - VD221D - VD222D - VD223D	V1.02 or later	1920 x 1080	448 x 252
-FD220D - CB220	V1.03 or later		
-CA220 -CAW220	V1.15 or later		
-UBX2301 Series	V2.04 or later		
-UBL2411 -UBL2401 Series	V2.05 or later		
-BX320D Series	V1.00 or later	2048 x 1536	320 x 240
-BX3400 Series	V1.15 or later		
-MFD320	V1.05 or later		
-BX320D-E - MDR320	V1.07 or later		
-BL320D - VD320D - VD321D - VD322D - VD323D	V1.02 or later		
-FD320D	V1.03 or later		
-UBX3301 Series	V2.04 or later		
-UBL3411 -UBL3401 Series	V2.05 or later		
-BX520D - MFD520	V1.05 or later	2560 x 1920	320 x 240
-BX5300-6V	V1.15 or later		
-BX520D-E - MDR520	V1.07 or later		
-PTZ010D-N	V1.07 or later	704 x 480	352 x 240
-PTZ010D-P	V1.07 or later	704 x 576	325 x 288